astaro security linux

Bedienungshandbuch

- Installation
- WebAdmin

Handbuch für
Astaro Security Linux V4

(Version 4.021)

Stand: 15.04.2004

Die in dieser Dokumentation enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Namen und Daten sind frei erfunden, soweit nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis der Astaro AG darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.

© Astaro AG. Alle Rechte vorbehalten.
Pfinztalstrasse 90, 76227 Karlsruhe, Germany
http://www.astaro.com

Portions © Kaspersky Labs.

Astaro Security Linux und WebAdmin sind Markenzeichen der Astaro AG. Linux ist ein Markenzeichen von Linus Torvalds. Alle weiteren Markenzeichen stehen ausschließlich den jeweiligen Inhabern zu.

Einschränkung der Gewährleistung

Für die Richtigkeit des Inhalts dieses Handbuchs wird keine Garantie übernommen. Hinweise auf Fehler und Verbesserungen nehmen wir gerne unter der E-Mail-Adresse documentation@astaro.com entgegen.

Inhaltsverzeichnis

Inhaltsverzeichnis **5**

1. Willkommen bei Astaro **9**

2. Einführung in die Technologie **10**

3. Installation **17**

3.1. Systemvoraussetzungen **18**

3.2. Installationsanleitung **21**

3.2.1. Software installieren **21**

3.2.2. Internet-Sicherheitssystem konfigurieren **26**

4. WebAdmin-Werkzeuge **33**

4.1. Info-Box/WebAdmin-Darstellung **33**

4.1.1. Info-Box **33**

4.1.2. WebAdmin-Darstellung **34**

4.2. Das Verzeichnis **34**

4.3. Menü **35**

4.3.1. Die Statusampel **35**

4.3.2. Die Auswahlfelder **35**

4.3.3. Das Drop-down-Menü **37**

4.3.4. Das Hierarchiefeld **37**

4.4. Online-Hilfe **39**

5. System bedienen & beobachten **40**

5.1. Grundeinstellungen (System) **42**

5.1.1. Settings **42**

5.1.2. Licensing **49**

5.1.3. Up2Date Service **52**

5.1.4. Backup **59**

5.1.5. Syslog 65
5.1.6. User Authentication..... 66
5.1.6.1. RADIUS 67
5.1.6.2. SAM – NT/2000/XP 71
5.1.6.3. LDAP Server 73
5.1.7. WebAdmin Site Certificate..... 86
5.1.8. High Availability 89
5.1.9. Shut down/Restart..... 94

5.2. Netzwerke und Dienste (Definitions) 96
5.2.1. Networks..... 96
5.2.2. Network Groups 97
5.2.3. Services..... 99
5.2.4. Service Groups 101
5.2.5. Users..... 102

5.3. Netzwerkeinstellungen (Network) 104
5.3.1. Interfaces 104
5.3.1.1. Standard Ethernet Interface..... 108
5.3.1.2. Additional address on ethernet interface 110
5.3.1.3. Wireless LAN 112
5.3.1.4. Virtual LAN 122
5.3.1.5. PPPoE-DSL-Verbindung 125
5.3.1.6. PPTPoE/PPPoA-DSL-Verbindung 128
5.3.1.7. Advanced Options 131
5.3.2. Routing 133
5.3.3. NAT/Masquerading 134
5.3.3.1. NAT 134
5.3.3.2. Masquerading..... 138
5.3.3.3. Load Balancing 140
5.3.4. DHCP Server..... 142
5.3.5. Portscan Detection 145
5.3.6. PPTP Roadwarrior Access..... 148

5.3.7. Quality of Service (QoS) 154
5.3.8. Accounting 158
5.3.9. Connection Tracking 160
5.3.10. Tools 160
5.4. Paketfilter (Packet Filter) 164
5.4.1. Rules 164
5.4.2. ICMP 170
5.4.3. Filter Live Log 172
5.5. Application Gateways (Proxies) 174
5.5.1. HTTP/Surf Protection 174
5.5.2. DNS 183
5.5.3. SOCKS 185
5.5.4. POP3 187
5.5.5. Ident 189
5.5.6. SMTP 190
5.5.6.1. Antispam/Content Control 195
5.5.7. Proxy Content Manager 205
5.6. Virtual Private Networks (IPSec VPN) 209
5.6.1. Connections 217
5.6.2. Policies 223
5.6.3. Local Keys 227
5.6.4. Remote Keys 229
5.6.5. CA Management 232
5.7. System Management (Reporting) 237
5.7.1. Hardware 237
5.7.2. Network 238
5.7.3. HTTP Proxy Cache 239
5.7.4. HTTP Proxy Usage 240
5.7.5. Accounting 241
5.7.6. Packet Filter 242

5.8. Log Files (Log Files) 244
5.8.1. Kernel 245
5.8.2. SMTP Relay 245
5.8.3. HTTP Proxy 246
5.8.4. Packet Filter 246
5.8.5. PPTP Roadwarrior Access 246
5.8.6. IPSec VPN 246
5.8.7. Daemon 246
5.8.8. Selfmonitor 247
5.8.9. Portscan 247
5.8.10. Admin Access 248
5.8.11. Notification 248
5.8.12. Accounting 257
5.8.13. WELF 258
5.8.14. POP3 258
5.9. Die Hilfe-Funktionen (Help) 259
5.10. Firewall verlassen (Exit) 260
6. Zusätzliche Funktionen 261
6.1. Serielle Konsole 261
6.2. Factory Reset 263
Glossar 265
Index 271

1. Willkommen bei Astaro

Wir begrüßen Sie herzlich als neuen Kunden unseres Internet-Sicherheitssystems Astaro Security Linux V4.

Dieses Handbuch führt Sie schrittweise durch die Installation des Internet-Sicherheitssystems, erklärt Ihnen ausführlich die Bedienung des Internet-Sicherheitssystems durch das web-basierte Konfigurationstool WebAdmin™ und unterstützt Sie bei der Dokumentation Ihrer Konfiguration.

Wenn Sie nicht sicher sind, ob Sie die aktuelle Version dieses Handbuchs vorliegen haben, können Sie diese unter folgender Internetadresse herunterladen:

http://docs.astaro.org

Um Sie über aktuelle Informationen und Neuerungen auf dem Laufenden zu halten, beinhaltet dieses Handbuch auch Verweise auf Internetadressen von Astaro sowie weiteren Anbietern. Diese Internetadressen können sich allerdings auch ändern, bzw. im Falle der Fremdanbieter auch ganz entfallen.

Sollten Sie Fragen haben oder Fehler im Handbuch entdecken, zögern Sie bitte nicht und kontaktieren uns unter folgender E-Mail-Adresse:

documentation@astaro.com

Wenden Sie sich für weitere Informationen an unser User-Forum unter der Internetadresse ...

http://www.astaro.org

... oder greifen auf die Astaro Support Angebote zurück.

2. Einführung in die Technologie

Bevor auf die Funktionsweise und Handhabung dieses Internet-Sicherheitssystems eingegangen wird, möchten wir Ihnen einen Einblick geben warum ein derartiges System zum Schutz des Netzwerks erforderlich ist und welche Probleme und Gefahren ohne ein entsprechendes Sicherheitssystem bestehen.

Netzwerke

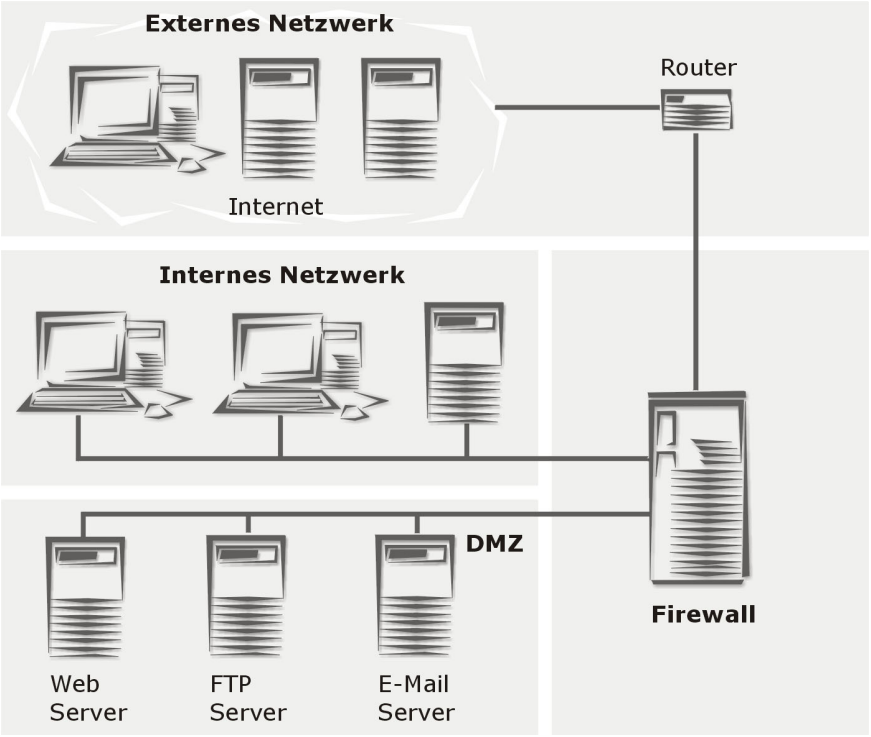
Das Internet ist heute als Schlüsseltechnologie für Kommunikation, Informationsbeschaffung, als Speichermedium für Wissens- und Erfahrungswerte sowie als Marktplatz für Informationsdienste etabliert. Seit seinen Anfängen haben sich seine Ausmaße vervielfacht und von 1995 bis 2002 war das zahlenmäßige Wachstum allein der .de-Domains nahezu exponential.

Die Endsysteme im weltumspannenden Netzwerk kommunizieren über das **Internet Protocol (IP)** und verschiedene andere Protokolle, die darauf aufsetzen z. B. TCP, UDP, ICMP. Basis einer solchen Kommunikation sind die IP-Adressen mit der Fähigkeit, alle erreichbaren Einheiten im Netzwerk eindeutig zu identifizieren.

Das Internet selbst existiert als Zusammenschluss verschiedenartiger Netzwerke, die sich sowohl durch die verwendeten Protokolle als auch durch die Ausbreitung unterscheiden. An Knotenpunkten, die zwei oder mehrere Netzwerke miteinander verbinden, entstehen eine Vielzahl von Aufgaben, die von Routern, Bridges oder Gateways übernommen werden. Ein spezieller Fall eines solchen Knotenpunktes ist die Firewall.
Hier treffen in aller Regel drei Typen von Netzwerken aufeinander:

- Externes Netzwerk/Wide Area Network (WAN)
- Internes Netzwerk/Local Area Network (LAN)
- De-Militarized Zone (DMZ)

Eine Beispiel-Konfiguration sehen Sie auf der nächsten Seite.



Die Firewall

Ein Modul dieses Internet-Sicherheitssystems ist die Firewall. Die charakteristischen Aufgaben einer Firewall als Schnittstelle zwischen WAN, LAN und DMZ sind:

- Schutz vor unbefugten Zugriffen
- Zugangskontrolle (wer darf wie und worauf zugreifen)
- Beweissicherheit gewährleisten
- Protokollauswertung durchführen
- Alarmierung bei sicherheitsrelevanten Ereignissen
- Verbergen der internen Netzstruktur
- Entkopplung von Servern und Clients durch Proxies
- Vertraulichkeit/Abhörsicherheit von Daten gewährleisten

Es existieren nun mehrere generische Netzwerkeinrichtungen, die unter dem Überbegriff **Firewall** zusammengefasst, diese Aufgaben übernehmen. Im Folgenden soll kurz auf einige Formen und ihre Ableger eingegangen werden:

Netzwerkschicht-Firewalls: Paketfilter (Packet Filter)

Wie der Name schon sagt, werden hier IP-Pakete (bestehend aus Adressinformation, einigen Flags und den Nutzdaten) gefiltert. Mit einer solchen Firewall können Sie, basierend auf verschiedenen Variablen, Zugang gewähren oder ablehnen. Diese Variablen sind u. a.:

- die Ursprungsadresse
- die Zieladresse
- das Protokoll (z. B. TCP, UDP, ICMP)
- die Port-Nummer

Dieser Ansatz bietet große Vorteile: Seine Geschwindigkeit bei der Bearbeitung der Pakete und er ist betriebssystem- und applikationsneutral.

In der fortgeschrittenen und komplexeren Entwicklungsform umfasst der Leistungsumfang von Paketfiltern die Interpretation der Pakete auf höherer Kommunikationsebene. In diesem Fall werden Pakete auch auf Transportebene (TCP/UDP) interpretiert und Statusinformationen für jede aktuelle Verbindung werden bewertet und festgehalten. Dieses Vorgehen wird als **Stateful Inspection** bezeichnet.

Der Paketfilter merkt sich den Zustand jeder einzelnen Verbindung und lässt nur Pakete passieren, die dem aktuellen Verbindungszustand entsprechen. Besonders interessant ist diese Tatsache für Verbindungsaufbauten vom geschützten in das ungeschützte Netzwerk:

Baut ein System im geschützten Netzwerk eine Verbindung auf, so lässt der **Stateful Inspection Packet Filter** z. B. Antwortpakete des externen Hosts in das geschützte Netzwerk passieren. Wird diese Verbindung wieder abgebaut, so hat kein System aus dem ungeschützten Netzwerk die Möglichkeit, Pakete in ihrem abgesicherten Netzwerk zu platzieren - es sei denn, Sie wollen es so und erlauben diesen Vorgang explizit.

Anwendungsschicht-Gateways: Application Proxy Firewall (Application Gateway)

Die zweite maßgebende Art von Firewalls sind die Anwendungsschicht-Gateways. Sie nehmen Verbindungen zwischen außenstehenden Systemen und Ihrem Netzwerk stellvertretend an. In diesem Fall werden Pakete nicht weitergeleitet, sondern es findet eine Art Übersetzung statt, mit dem Gateway als Zwischenstation und Übersetzer.

Die Stellvertreterprozesse auf dem Application Gateway werden als **Proxyserver** oder kurz **Proxies** bezeichnet. Jeder Proxy kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsmerkmale anbieten. Es ergeben sich weitere umfangreiche Sicherungs- und Protokollierungsmöglichkeiten durch die Verwendung von **Proxies**.

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten jeweils klar durch Protokollstandards definiert ist. Die Proxies konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine überschaubare Module verwendet werden, wodurch die Fehleranfälligkeit durch Implementationsfehler reduziert wird.

Bekannte Proxies sind z. B.:

- HTTP-Proxy mit Java, JavaScript & ActiveX-Filter
- SMTP-Proxy, verantwortlich für die Zustellung von E-Mails und für das Überprüfen auf vorhandene Viren
- SOCKS-Proxy als generischer, authentifizierungssfähiger Circuit-Level-Proxy

Der Vorteil der Anwendungsschicht-Gateways ist, dass das gesicherte Netzwerk physikalisch und logisch vom ungesicherten Netzwerk getrennt wird. Sie stellen sicher, dass kein Paket direkt zwischen den Netzwerken fließen kann. Direktes Resultat daraus ist ein reduzierter Administrationsaufwand. Sie stellen lediglich die Integrität der Stellvertreter sicher und schützen damit sämtliche Clients und Server in Ihrem Netzwerk - unabhängig von Marke, Programmversion oder Plattform.

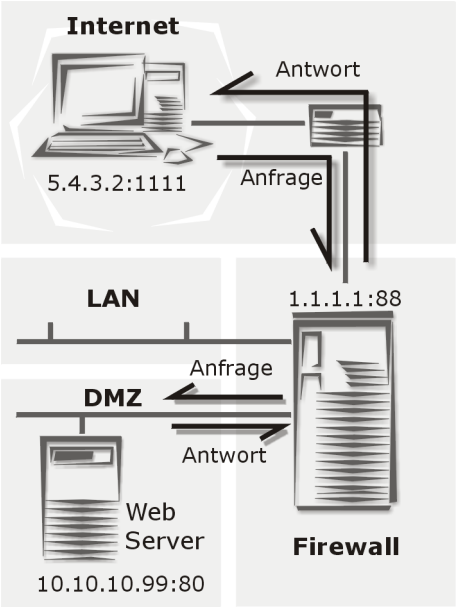
Schutzmechanismen

Weitere Mechanismen gewährleisten zusätzliche Sicherheit:

Die Verwendung privater IP-Adressen in den geschützten Netzwerken, gepaart mit **Network Address Translation (NAT)** in den Ausprägungen

- Masquerading
- Source NAT (SNAT)
- Destination NAT (DNAT)

erlaubt es, ein gesamtes Netzwerk hinter einer oder wenigen offiziellen IP-Adressen zu verbergen und die Erkennung Ihrer Netztopologie von außen zu verhindern.



Bei nach wie vor voll verfügbarer Internet-Konnektivität ist nach außen hin keine Identifikation von Endsystemen mehr möglich.

Durch **Destination NAT** ist es trotzdem möglich, Server innerhalb des geschützten Netzwerks oder der DMZ zu platzieren und für einen bestimmten Dienst nach außen hin verfügbar zu machen.

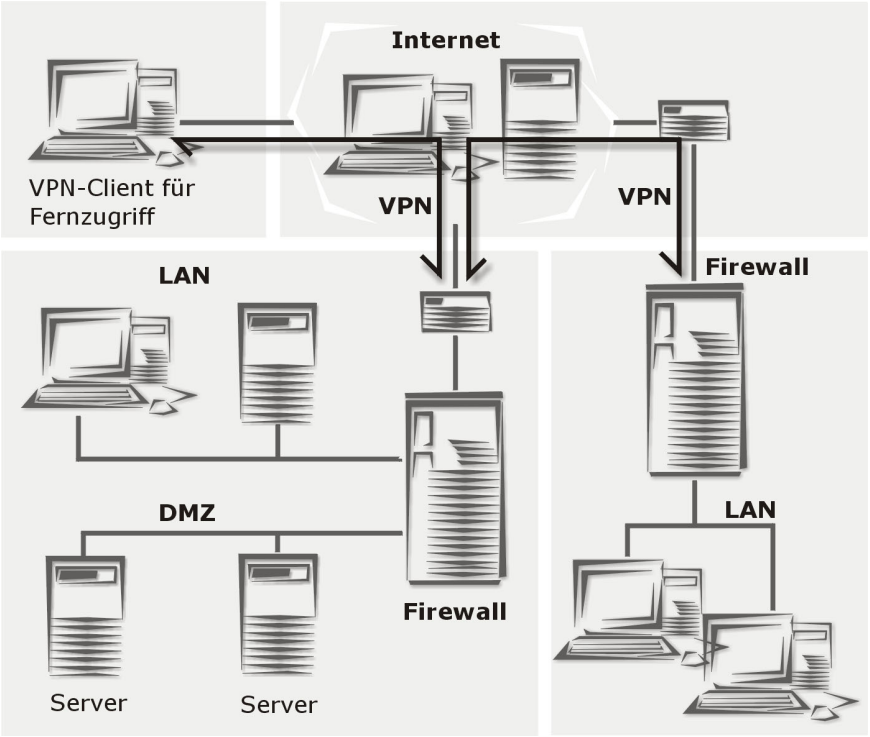
Beispiel: Ein Benutzer (wie in der linken Grafik dargestellt) mit der IP-Adresse 5.4.3.2, Port 1111 schickt eine Anfrage an den Web-Server in der DMZ. Er kennt nur die externe IP-Adresse (1.1.1.1, Port 88).
Durch **DNAT** ändert nun die Firewall die Zieladresse der Anfrage in 10.10.10.99, Port 80 und schickt diese an den Web-Server. Der Web-Server schickt anschließend die Antwort mit seiner internen IP-Adresse (10.10.10.99, Port: 80) und der IP-Adresse des Benutzers ab. Die Firewall erkennt das Paket anhand der Benutzeradresse und ändert nun die Quelladresse von der

internen IP- (10.10.10.99, Port 80) in die externe IP-Adresse (1.1.1.1, Port 88).

Die Geschäftswelt stellt heute Anforderungen an die IT-Infrastruktur, zu denen Echtzeit-Kommunikation und enge Zusammenarbeit mit Geschäftspartnern, Consultants und Zweigstellen gehören. Die Forderung nach Echtzeitfähigkeit führt immer öfter zur Schöpfung so genannter Extranets, die mit dem Netzwerk des Unternehmens entweder ...

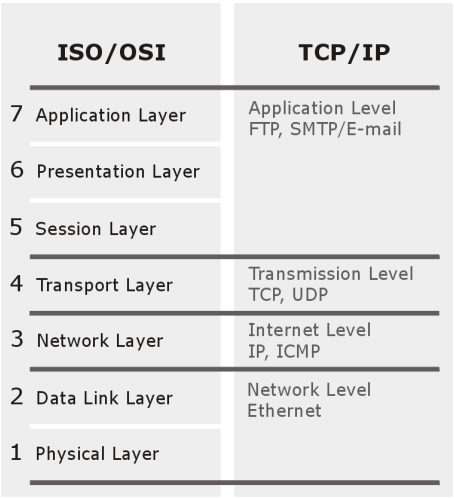
- über dedizierte Standleitungen, oder
- unverschlüsselt über das Internet

... erfolgen. Dabei hat jede dieser Vorgehensweisen Vor- und Nachteile, da ein Konflikt zwischen den entstehenden Kosten und den Sicherheitsanforderungen auftritt.



Durch **Virtual Private Network (VPN)** wird es möglich, abgesicherte, d. h. verschlüsselte Verbindungen zwischen LANs aufzubauen, die transparent von Endpunkt zu Endpunkt über das Internet geleitet werden. Dies ist insbesondere sinnvoll, wenn Ihre Organisation an mehreren Standpunkten operiert, die über eine Internet-Anbindung verfügen. Aufbauend auf dem IPSec-Standard wird es hier möglich, sichere Verbindungen herzustellen.

Unabhängig von der Art der zu übertragenden Daten wird diese verschlüsselte Verbindung automatisch (d. h. ohne die Notwendigkeit zusätzlicher Konfigurationen oder Passwörter am Endsystem) genutzt, um den Inhalt während des Transports abzusichern.



Am anderen Ende der Verbindung werden die übermittelten Daten wieder transparent entschlüsselt und stehen in ihrer ursprünglichen Form dem Empfänger zur Verfügung.

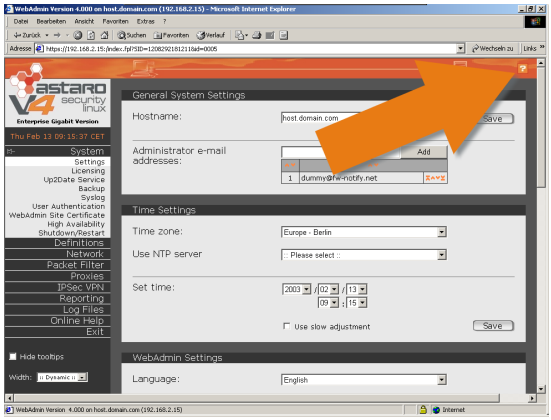
Die **Firewall** dieses Internet-Sicherheitssystems ist ein Hybrid aus den genannten Schutzmechanismen und vereinigt die Vorteile aller Varianten:

Die **Stateful Inspection Packet Filter**-Funktionalität bietet plattformunabhängig die nötige Flexibilität, um alle nötigen Dienste definieren, freischalten oder sperren zu können.
Vorhandene **Proxies** machen **Astaro Security Linux** zum **Application Gateway**, der die wichtigsten Endsystem-Dienste wie **HTTP**, **Mail** und **DNS** durch Stellvertreter absichert und zudem durch SOCKS generisches Circuit-Level-Proxying ermöglicht.

VPN, **SNAT**, **DNAT**, **Masquerading** und die Möglichkeit, **statische Routen** zu definieren, erweitern die dedizierte Firewall zu einem leistungsfähigen Knoten- und Kontrollpunkt in Ihrem Netzwerk.

3. Installation

Die Installation des Internet-Sicherheitssystems gliedert sich in zwei Teile. Der erste Teil beinhaltet das Einspielen der Software - dies führen Sie im **Installationsmenü** durch. Der zweite Teil ist die Konfiguration des Internet-Sicherheitssystems und erfolgt im web-basierten Konfigurationstool **WebAdmin** von Ihrem Arbeitsplatz aus.



Hinweise zur Funktionalität des **WebAdmin** entnehmen Sie der **Online Help**. Die Hilfe wird über die Schaltfläche **?** geöffnet. Zur Zeit ist die Online Hilfe nur in englischer Sprache verfügbar.

Auf den folgenden Seiten können Sie die Daten zur Konfiguration (z. B. das Default Gateway und die IP-Adressen der installierten Netzwerkkarten) in die entsprechenden Felder eintragen und anschließend archivieren.

Achtung:

Falls Sie Ihr Internet-Sicherheitssystems von Version 3.2x auf Version 4.0 aktualisieren und die bestehende Konfiguration übernehmen wollen, müssen Sie zuvor Ihr bestehendes System mindestens auf Version 3.216 updaten. Weitere Informationen zum Up2Date-Service und zur Backup-Funktion erhalten Sie in den Kapiteln 5.1.3 und 5.1.4.

3.1. Systemvoraussetzungen

Damit Sie das Internet-Sicherheitssystem auf Ihrer Hardware installieren können, müssen die nachfolgenden Voraussetzungen erfüllt sein:

Hardware

- Prozessor: Pentium II oder kompatibel
- 128 MB Arbeitsspeicher
- 8 GB IDE oder SCSI Festplatte
- Bootfähiges IDE oder SCSI CD-ROM-Laufwerk
- 2 oder mehr PCI Ethernet Netzwerkkarten
- Für die Schnittstelle zu einem Wireless LAN: Wireless-LAN-PCMCIA-Karte mit Prism2-Chipsatz oder kompatibel

Wichtiger Hinweis:

Für das **High Availability (HA)**-System und zur Konfiguration einer Schnittstelle zum **Wireless LAN** oder einem **Virtual LAN** benötigen Sie Hardware, die vom Internet-Sicherheitssystem für die entsprechende Funktion unterstützt wird. Die Hardware ist unter der Internetadresse **http://docs.astaro.org** im Verzeichnis **Hardware Compatibility List for Astaro Security Linux** aufgelistet.

Zur einfacheren Konfiguration des **High Availability (HA)**-Systems mit Überwachung mittels Heart Beat empfiehlt es sich für alle Schnittstellen link-beat-fähige Netzwerkkarten zu verwenden. Die Installation des **HA**-Systems wird in Kapitel 5.1.8 ab Seite 89 beschrieben.

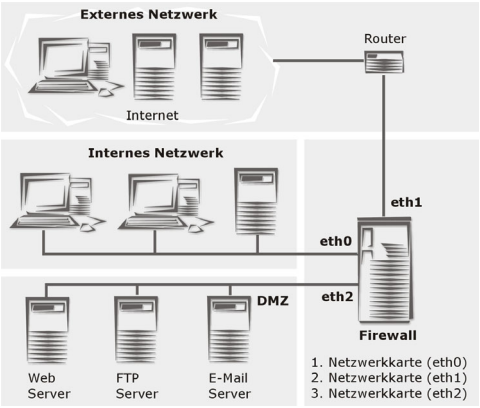
Administrations-PC

- Korrekte Konfiguration der **IP-Adresse**, der **Subnetzwerkmaske** und des **Default Gateway**
- Ein HTTPS-fähiger Browser (Microsoft Explorer 5.0 oder höher, Netscape Communicator 6.1 oder höher oder Mozilla 1.0+):

  Im Browser müssen **JavaScript** und **Cascading Style Sheets** aktiviert sein.

  Die IP-Adresse der internen Netzwerkkarte (eth0) muss im Browser von der Verwendung eines Proxyservers ausgeschlossen sein

Beispielkonfiguration



Das Internet-Sicherheitssystem sollte, wie in der linken Konfiguration dargestellt, die einzige Verbindung zwischen Ihrem internen (LAN) und dem externen Netzwerk (Internet) herstellen.

Adresstabelle

	IP-Adresse	Netzwerkmaske	Default Gateway
Mit internem Netzwerk verbundene Netzwerk-karte	___.___.___.___	___.___.___.___	___.___.___.___
Mit extern-em Netz-werk ver-bundene Netzwerk-karte	___.___.___.___	___.___.___.___	
Mit DMZ verbundene Netzwerk-karte [1)]	___.___.___.___	___.___.___.___	
Netzwerk-karte für HA-System[2)]	___.___.___.___	___.___.___.___	

[1)] Die dritte und weitere Netzwerkkarten sind optional.

[2)] Netzwerkkarte für High Availability (HA).

3.2. Installationsanleitung

Ab hier werden Sie schrittweise durch die Installation geführt.

Achtung:

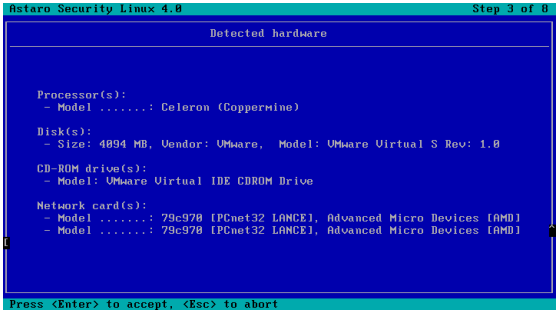
Bei der Installation der Software werden alle bestehenden Daten auf dem Rechner gelöscht!

Vorbereitung

Bitte legen Sie vor der Installation folgende Unterlagen bereit:

- Internet-Sicherheitssystem CD-ROM
- die ausgefüllte Adresstabelle mit den zu verwendenden **IP-Adressen** und den **Netzmasken** sowie die IP-Adresse des **Default Gateway**

3.2.1. Software installieren


Astaro Security Linux 4.0
Step 3 of 8
Detected hardware
Processor(s):
- Model .....: Celeron (Coppermine)
Disk(s):
- Size: 4094 MB, Vendor: VMware, Model: VMware Virtual S Rev: 1.0
CD-ROM drive(s):
- Model: VMware Virtual IDE CDROM Drive
Network card(s):
- Model .....: 79c970 [PCnet32 LANCE], Advanced Micro Devices [AMD]
- Model .....: 79c970 [PCnet32 LANCE], Advanced Micro Devices [AMD]
Press <Enter> to accept, <Esc> to abort

Den ersten Teil der Installation führen Sie im Installationsmenü durch (linkes Bild).

Zuerst erfolgt ein Hardware-Check. Anschließend geben Sie über den Dialog die Daten ein und danach wird die Software auf Ihrem PC eingespielt.

Hinweis:

Falls Ihr SCSI-Adapter nicht unterstützt wird, wenden Sie sich bitte an den Support Ihres Sicherheitssystem-Anbieters.

Achtung:

Falls Sie diese Installation aufgrund einer Änderung der Hardwarekonfiguration, z. B. durch das Hinzufügen oder Entfernen von Netzwerkkarten, durchführen möchten, wenden Sie sich an den Support Ihres Sicherheitssystem-Anbieters. In besonderen Fällen ist eine Neuinstallation nicht notwendig.

1. PC von der CD-ROM booten (Schritt 1):

   Die Navigation im Installationsmenü erfolgt über die nachfolgenden Tasten. Beachten Sie während der Installation auch die zusätzlichen Tastenfunktionen in der grünen Fußleiste.

   Cursor-Tasten: Navigation in den Texten, z. B. in den Lizenzbestimmungen und zur Auswahl des Keyboard-Layouts.

   Enter-Taste: Die Eingabe wird bestätigt und zum nächsten Punkt fortgefahren.

   ESC-Taste: Abbruch der Installation.

   Tab-Taste: Wechseln zwischen den Text- und Eingabefeldern sowie den Schaltflächen.

   Achtung:

   Bei der Installation der Software werden alle bestehenden Daten auf dem PC gelöscht!

2. Keyboard-Layout (Schritt 2):

   Wählen Sie mit den **Cursor**-Tasten das Keyboard-Layout aus und bestätigen Sie dies mit der **Enter**-Taste.

3. Hardware-Test (Schritt 3):

   Die Software prüft die folgenden Hardware-Komponenten: Prozessor, Fabrikat und Größe der Festplatte, CD-ROM-Laufwerk, Netzwerkkarten sowie den IDE- bzw. SCSI-Controller.
   Falls die vorhandenen Hardware-Ressourcen zur Installation der Software nicht ausreichen, wird die Installation mit der entsprechenden Fehlermeldung abgebrochen.

4. Lizenzbestimmungen (Schritt 4):

Hinweis:

Beachten Sie die rechtlichen Hinweise und Lizenzbestimmungen.

Die Lizenzbestimmungen akzeptieren Sie mit der **F8**-Taste.

5. Datum und Uhrzeit (Schritt 5):

   Wählen Sie mit den **Cursor**-Tasten das Land aus und bestätigen Sie dies mit der **Enter**-Taste.

   Wählen Sie mit den **Cursor**-Tasten die Zeitzone aus und bestätigen Sie dies mit der **Enter**-Taste.

   Tragen Sie anschließend in die Eingabefelder das aktuelle Datum und die Uhrzeit ein. Sie können mit der **Tab**-Taste und den **Cursor**-Tasten zwischen den Eingabefeldern wechseln. Ungültige Eingaben werden nicht übernommen.
   Bestätigen Sie die Eingaben mit der **Enter**-Taste.

6. Netzwerkkarte auswählen und konfigurieren (Schritt 6):

   Damit Sie nach der Software-Installation das Internet-Sicherheitssystem mit dem Tool **WebAdmin** konfigurieren können, müssen Sie eine Netzwerkkarte definieren. Diese Netzwerkkarte ist später die **interne Netzwerkkarte (eth0)**.
   Wählen Sie aus den verfügbaren Netzwerkkarten eine aus und bestätigen Sie die Auswahl mit der **Enter**-Taste.

   Definieren Sie anschließend für diese Netzwerkkarte die **IP-Adresse**, die **Netzwerkmaske** und das **Gateway** (Default Gateway).

   Beispiel:

   Address: 192.168.2.100

   Netmask: 255.255.255.0

   Das **Gateway** müssen Sie eingeben, wenn Sie mit einem PC auf das Konfigurationstool **WebAdmin** zugreifen möchten, der außerhalb des Netzwerkbereichs liegt. Beachten Sie dabei, dass das Gateway innerhalb des Netzwerkbereichs liegen muss.

Bei der Netzwerkmaske 255.255.255.0, wird das Sub-Netzwerk durch die ersten drei Werte definiert. In unserem Beispiel lautet der relevante Bereich 192.168.2. Wenn nun Ihr Administrations-PC z. B. die IP-Adresse 192.168.10.5 hat, liegt er nicht im selben Sub-Netzwerk und in diesem Fall benötigen Sie ein Gateway. Für unser Beispiel nehmen wird die folgende Adresse:

Gateway: 192.168.2.1

Falls der Administrations-PC innerhalb des Netzwerkbereichs liegt, geben Sie den folgenden Wert ein:

Gateway: none

Bestätigen Sie die Eingaben mit der **Enter**-Taste.

7. Abschließende Hinweise (Schritt 7):

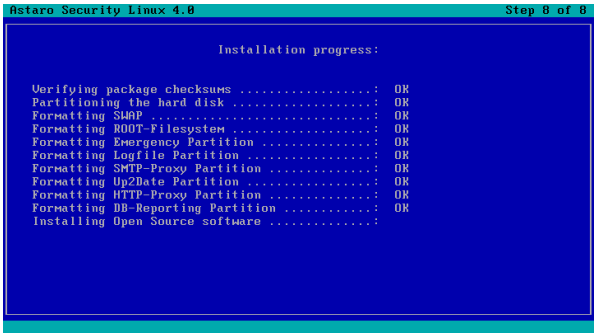
Achtung:

Beachten Sie die abschließenden Hinweise zur Installation der Software. Nach Bestätigung des Warnhinweises werden alle bestehenden Daten auf dem PC gelöscht!

Falls Sie Eingaben ändern möchten, können Sie nun mit der **F12**-Taste wieder zu Schritt 1 des Installationsmenüs gelangen.
Sie starten die Installation der Software mit der **Enter**-Taste.

8. Software installieren (Schritt 8):

Die Installation der Software kann nun einige Minuten dauern. Sie können den Installationsvorgang mit Hilfe von vier Konsolen verfolgen.


Astaro Security Linux 4.0
Step 8 of 8
Installation progress:
Verifying package checksums ..... : OK
Partitioning the hard disk ..... : OK
Formatting SWAP ..... : OK
Formatting ROOT-Filesystem ..... : OK
Formatting Emergency Partition ..... : OK
Formatting Logfile Partition ..... : OK
Formatting SMTP-Proxy Partition ..... : OK
Formatting Up2Date Partition ..... : OK
Formatting HTTP-Proxy Partition ..... : OK
Formatting DB-Reporting Partition ..... : OK
Installing Open Source software ..... :

Die vier Konsolen:

Install-Routine (**Alt** + **F1**).

Interaktive **Bash**-Shell (**Alt** + **F2**).

Log-Ausgabe der Install-Routine (**Alt** + **F3**).

Kernel-Ausgabe (**Alt** + **F4**).

Sobald Sie dazu aufgefordert werden, entnehmen Sie die CD-ROM aus dem Laufwerk und verbinden die Netzwerkkarte **eth0** mit Ihrem lokalen Netzwerk.

Mit Ausnahme der **internen Netzwerkkarte (eth0)** wird die Reihenfolge der Netzwerkkarten in erster Linie durch die **PCI ID** und den **Kernel**-Treiber bestimmt.
Die Reihenfolge der Netzwerkkartenbenennung kann sich auch später durch Änderung der Hardwarekonfiguration, z. B. durch das Hinzufügen oder Entfernen von Netzwerkkarten und der damit verbundenen Neuinstallation ändern.

9. Internet-Sicherheitssystem neu starten

   Starten Sie das Internet-Sicherheitssystem mit der Tastenkombination **Strg** + **Alt** + **Entf** oder durch **Reset** neu.

   Während des Boot-Vorgangs wird die IP-Adresse der internen Netzwerkkarte neu gesetzt, daher kann auf der Konsole **Install-Routine** (**Alt** + **F1**) für kurze Zeit die Meldung `No IP on eth0` angezeigt werden.

Nachdem das Internet-Sicherheitssystem neu gestartet ist (je nach Hardware dauert dies bis zu fünf Minuten), sollten Sie mittels **Ping** die IP-Adresse der **eth0**-Netzwerkkarte erreichen.

Falls keine Verbindung zustande kommt, prüfen Sie bitte Ihr System auf die nachfolgenden möglichen Fehlerquellen.

Fehler: Sie erreichen das Internet-Sicherheitssystem nicht vom lokalen Netzwerk.

Mögliche Fehlerursachen:

- IP-Adresse des Internet-Sicherheitssystems ist nicht korrekt gesetzt
- IP-Adresse am Client-Rechner ist nicht korrekt gesetzt
- Default Gateway am Client-Rechner ist nicht korrekt gesetzt
- Netzwerkkabel steckt in der falschen Netzwerkkarte
- Alle Netzwerkkarten des Internet-Sicherheitssystems sind an einem Hub angeschlossen

Hinweis:

Falls Sie für Ihre Verbindung zum Internet **DSL** verwenden, beachten Sie bei der Konfiguration den entsprechenden Leitfaden unter der Internetadresse **http://docs.astaro.org**.

3.2.2. Internet-Sicherheitssystem konfigurieren

Die Konfiguration des Internet-Sicherheitssystems führen Sie von Ihrem Administrations-PC aus mit einem Internet Browser (z. B. MS Internet Explorer) und dem Konfigurationstool **WebAdmin** durch:

1. Browser starten und **WebAdmin** öffnen

   Bevor Sie das Konfigurations-Tool **WebAdmin** öffnen können, müssen Sie den Browser entsprechend konfigurieren. Weitere Informationen erhalten Sie in Kapitel 5.5.1 ab Seite 174.

   Wenn der Browser konfiguriert ist, geben Sie die IP-Adresse des Internet-Sicherheitssystems (eth0) wie folgt ein: **https://IP-Adresse**
   (Im Beispiel von Schritt 6 ist es https://192.168.2.100)

   Anschließend erscheint ein **Sicherheitshinweis**. Dieser Hinweis wird später nicht mehr angezeigt, wenn Sie für Ihre

WebAdmin-Seite ein CA-Zertifikat generieren.
Ausführliche Informationen zum Zertifikat und wie Sie dieses Zertifikat installieren, wird in Kapitel 5.1.7 ab Seite 86 beschrieben.

Bestätigen Sie die Frage auf dem **Sicherheitshinweis**, ob der Vorgang fortgesetzt werden soll, mit einem Klick auf die Schaltfläche **Ja**.

Beim ersten Start des **WebAdmin** öffnet sich ein Menü mit den Fenstern **License Agreement** und **Setting system passwords**.

2. Lizenzbestimmungen akzeptieren

   Die Lizenzbestimmungen im Fenster **License Agreement** akzeptieren Sie durch einen Klick auf das Optionsfeld **I agree to the terms of the license**.

Hinweis:

Beachten Sie die rechtlichen Hinweise und Lizenzbestimmungen.

3. Passwörter setzen

   Setzen Sie im Fenster **Setting system passwords** die Passwörter für das Internet-Sicherheitssystem.

Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35$4.
Beim **WebAdmin User**-Passwort sind nur die ersten acht Stellen signifikant.

Sie können **WebAdmin** nur starten, wenn Sie für die folgenden Funktionen ein Passwort gesetzt haben. Bestätigen Sie die Passwörter durch die nochmalige Eingabe in das jeweilige Eingabefeld **Confirm**. Der Benutzernamen (**Username**) ist vorgegeben und kann nicht geändert werden.

WebAdmin user: Zugang zum WebAdmin.
Der Benutzername lautet **admin**.

Shell Login user: Zugang via SSH.
Der Benutzername lautet **loginuser**.

Shell Administrator user: Administratorrechte für das gesamte Internet-Sicherheitssystem.
Der Benutzername lautet **root**.

Sicherheitshinweis:

Setzen Sie für **Shell Login** und **Shell Administrator** unterschiedliche Passwörter.

Astaro Configuration Manager User (optional): Dieses Passwort benötigen Sie, falls das Internet-Sicherheitssystem mit dem Astaro Configuration Manager konfiguriert werden soll.

Boot Manager (optional): Dieses Passwort verhindert, dass Unbefugte Änderungen in den Bootparametern vornehmen können.

Bestätigen Sie die gesetzten Passwörter durch einen Klick auf die Schaltfläche **Save**.

4. Im Konfigurations-Tool **WebAdmin** authentifizieren

   User: **admin**

   Password: Passwort des WebAdmin-Benutzers

   Beachten Sie bitte die Groß- und Kleinschreibung!

   Klicken Sie auf die Schaltfläche **Login**.

Hinweis:

Gehen Sie die Schritte 5 bis 15 in der angegebenen Reihenfolge durch.

5. Erste Grundeinstellungen durchführen

   Öffnen Sie im Verzeichnis **System** das Menü **Settings** und führen Sie im Fenster **General System Settings** folgende Einstellungen durch:

   Hostname: Tragen Sie hier den **Hostnamen** für Ihr Internet-Sicherheitssystem ein.
   Ein Domainname darf aus alphanumerischen Zeichen sowie Punkt- und Minus-Zeichen bestehen. Am Ende muss ein alphabetischer Bezeichner vorhanden sein, z. B. „com", „de" oder „org". Der **Hostname** wird in allen **Notification E-Mails** in der Betreffzeile angezeigt.

Administrator e-mail addresses: Tragen Sie in das Hierarchiefeld die E-Mail-Adresse des Administrators ein.

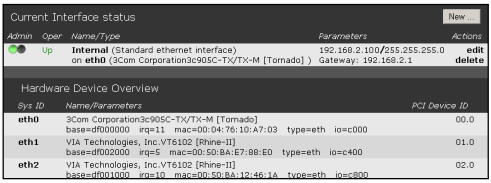
Weitere Informationen zu diesen Funktionen erhalten Sie in Kapitel 5.1.1 ab Seite 42.

Speichern Sie abschließend die Eingaben durch einen Klick auf die Schaltfläche **Save**.

6. Interne Netzwerkkarte (eth0) editieren

Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces** und prüfen Sie die Einstellungen der internen Netzwerkkarte (eth0).

Die Netzwerkkarte (eth0) zum internen Netzwerk wurde von Ihnen während der Installation der Software definiert. Diese Netzwerkkarte wird nach dem ersten Start des Internet-Sicherheitssystems im Fenster **Current Interface Status** angezeigt.



Falls Sie bei dieser Netzwerkkarte Einstellungen ändern möchten, z. B. einen anderen Namen, führen Sie diese jetzt durch. Um die Einstellungen zu editieren öffnen Sie das Menü **Edit Interface** durch einen Klick auf die Schaltfläche **edit**.

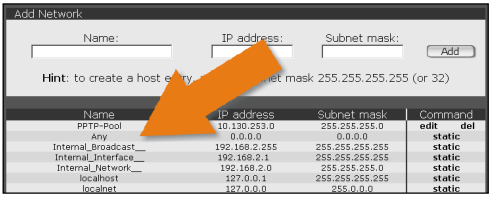
Achtung:

Wenn Sie die **IP-Adresse** der internen Netzwerkkarte **eth0** ändern, besteht die Möglichkeit, dass Sie sich "aussperren".

Die Konfiguration der Netzwerkarten und virtuellen Schnittstellen (**Interfaces**) wird in Kapitel 5.3.1 ab Seite 104 beschrieben.

7. Internes Netzwerk konfigurieren

   Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks** und prüfen Sie die Einstellungen für das interne Netzwerk. Während der Installation wurden vom Internet-Sicherheitssystem aufgrund Ihrer Definition der internen Netzwerkkarte (eth0) automatisch drei logische Netzwerke definiert:



   Die Schnittstelle **Internal_Interface__**, bestehend aus der von Ihnen definierten IP-Adresse (Beispiel: 192.168.2.1) und der Netzwerkmaske 255.255.255.255 (Host).

   Das interne Netzwerk **Internal_Network__**, bestehend aus der Netzwerk-IP-Adresse (Beispiel: 192.168.2.0) und der Netzwerkmaske (Beispiel: 255.255.255.0).

   Der Broadcast **Internal_Broadcast__**, bestehend aus der Broadcast-IP (Beispiel: 192.168.2.255) und der Netzwerkmaske 255.255.255.255 (Host).

   Das Definieren neuer Netzwerke (**Networks**) wird im Handbuch in Kapitel 5.2.1 ab Seite 96 beschrieben.

8. Externe Netzwerkkarte (eth1) konfigurieren

   Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces** und konfigurieren Sie die Schnittstelle zum externen Netzwerk (Internet). Die Wahl der Schnittstelle und die dafür notwendigen Einstellungen auf der externen Netzwerkkarte hängen von der Art des Internetzugangs ab.

   Die Konfiguration der Netzwerkarten und virtuellen Schnittstellen (**Interfaces**) wird in Kapitel 5.3.1 ab Seite 104 beschrieben.

9. Masquerading-Regel für das interne Netzwerk definieren

   Falls Sie in Ihrem Netzwerk private IP-Adressen verwenden möchten und eine direkte Verbindung ohne Proxy benötigen, setzen Sie unter dem Verzeichnis **Network** im Menü **NAT** die entsprechenden **Masquerading**-Regeln.

   Weitere Informationen zu **DNAT**, **SNAT** und **Masquerading** erhalten Sie im Kapitel 5.3.3 ab Seite 134.

Die IP-Routing-Einträge für an die Netzwerkkarten angeschlossene Netzwerke (**Interface Routes**) werden automatisch erstellt.
Bei Bedarf können Sie im Menü **Routing** IP-Routing-Einträge auch manuell definieren. Dies ist allerdings nur in komplexeren Netzwerken notwendig.

10. DNS-Proxy konfigurieren

    Öffnen Sie im Verzeichnis **Proxies** das Menü **DNS** und konfigurieren Sie den DNS-Proxy.

    Durch die Konfiguration des DNS-Proxy beschleunigen Sie die Namensauflösung. Sie können einen lokalen **Nameserver (DNS)** oder den Ihres Internet Service Providers eintragen. Andernfalls verwendet Ihr Internet-Sicherheitssystem automatisch die **Root-Nameserver**.

    Die Konfiguration des **DNS-Proxy** wird in Kapitel 5.5.2 ab Seite 183 beschrieben.

11. Weitere Netzwerke anschließen

    Falls noch weitere interne Netzwerke vorhanden sind, verbinden Sie diese mit den Netzwerkkarten des Internet-Sicherheitssystems.

12. HTTP-Proxy konfigurieren

    Falls Rechner im internen Netzwerk unter Verwendung des Proxies auf das Internet zuzugreifen sollen, öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP** und schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

    Die Konfiguration des **HTTP-Proxy** wird in Kapitel 5.5.1 ab Seite 174 beschrieben.

    Damit die Rechner im internen Netzwerk anschließend unter Verwendung des HTTP-Proxy auf das Internet zugreifen können, müssen die Browser entsprechend konfiguriert werden.

13. Die Paketfilterregeln setzen

    Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die Paketfilterregeln.

    Neue Regeln werden inaktiv an letzter Stelle angefügt und müssen dann einsortiert werden. Die Regeln werden von oben nach unten abgearbeitet, wobei die Verarbeitung

durch die erste zutreffende Regel beendet wird. Durch einen Klick auf die Statusampel wird die Regel aktiv (Statusampel zeigt Grün).
Beachten Sie, dass aufgrund von **Stateful Inspection** nur für den Verbindungsaufbau Paketfilterregeln gesetzt werden müssen. Die Antwort- oder Rückpakete werden automatisch erkannt und akzeptiert.
Das Setzen von Paketfilterregeln (**Packet Filter**) wird in Kapitel 5.4 ab Seite 164 beschrieben.

14. Paketfilter beobachten/Debugging

    Im Menü **Packet Filter/Filter Live Log** können Sie sehen, welche Datenpakete in Ihrem Paketfilter gefiltert werden.
    Wenn nach der Installation des Internet-Sicherheitssystems Probleme auftauchen, so eignen sich diese Informationen zum **Debugging** Ihrer Paketfilterregeln.

    Das Modul **Filter Live Log** wird in Kapitel 5.4.3 ab Seite 172 beschrieben.

15. Sicherheitssystem und Virenscanner aktualisieren

    Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service** und führen Sie das **System Up2Date** aus.

    Falls Ihre Lizenz auch **Virus Protection** beinhaltet, starten Sie anschließend manuell das Modul **Pattern Up2Date**.

    Das Modul **Up2Date Service** wird in Kapitel 5.1.3 ab Seite 52 beschrieben.

Wenn Sie diese Schritte erfolgreich durchgeführt haben, ist die Erstkonfiguration des Internet-Sicherheitssystems abgeschlossen. Schließen Sie nun das Konfigurationstool **WebAdmin** durch einen Klick auf die Schaltfläche **Exit**.

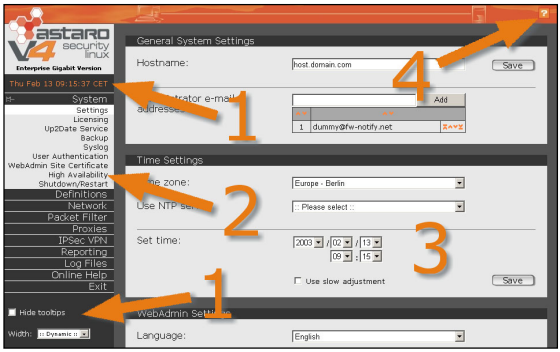
Probleme

Sollten bei der Durchführung dieser Schritte Probleme auftauchen, so wenden Sie sich bitte an den Support ihres Sicherheitssystem-Anbieters, oder besuchen Sie das **Astaro Bulletin Board** unter:

http://www.astaro.org

4. WebAdmin-Werkzeuge

Mit dem Konfigurationstool **WebAdmin** können Sie alle Einstellungen am Internet-Sicherheitssystem durchführen. In diesem Kapitel werden die Werkzeuge und Hilfsmittel von WebAdmin erläutert.



Das Konfigurationstool **WebAdmin** besteht aus vier Komponenten:

(1) Info-Box/Einstellung WebAdmin-Darstellung

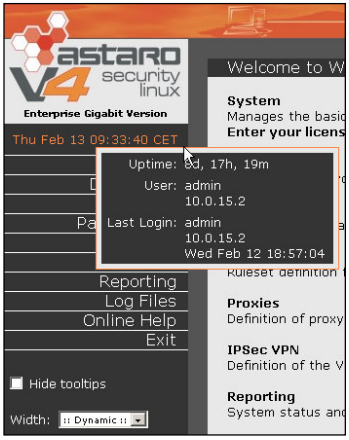
(2) Verzeichnis

(3) Menü

(4) Online-Hilfe

4.1. Info-Box/WebAdmin-Darstellung

4.1.1. Info-Box



In der linken oberen Ecke wird die von Ihnen erworbene Lizenz, die Systemzeit und die Zeitzone angezeigt. Die hinterlegte Info-Box wird geöffnet, wenn Sie mit der Maus die Zeitangabe berühren. Folgende Informationen werden angezeigt:

Uptime: Dokumentiert die Verfügbarkeit Ihres Internet-Sicherheitssystems, d. h. den Zeitraum seit dem das System ohne Unterbrechung verfügbar ist.

User: Zeigt an, welcher Benutzer von welchem Client aus gerade auf den **WebAdmin** zugreift.

Last Login: Zeigt an, wann und von welchem Client aus das letzte Mal auf den **WebAdmin** zugegriffen wurde.

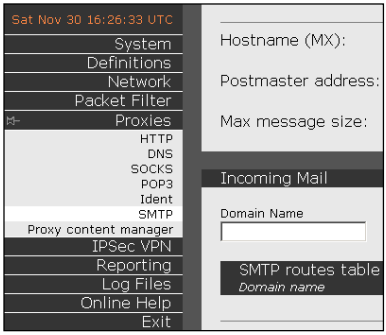
4.1.2. WebAdmin-Darstellung

Hide tooltips: Durch einen Klick auf das Optionsfeld werden die gelben Info-Anzeigen (Tooltips) in den Menüs ausgeschaltet.

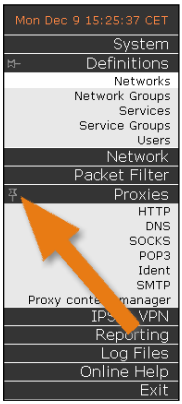
Width: In diesem Drop-down-Menü können Sie die Auflösung des **WebAdmin** Ihrem Monitor anpassen.
Mögliche Einstellungen sind **1024x768**, **800x600** und **Dynamic**.

Alle Einstellungen werden sofort übernommen.

4.2. Das Verzeichnis



Über das Verzeichnis gelangen Sie in die einzelnen Menüs, um das Internet-Sicherheitssystem zu administrieren. Damit Sie im Handbuch die entsprechende Funktionsbeschreibung schnell finden, entspricht das Kapitel 5 „System bedienen & beobachten" der Verzeichnisstruktur des WebAdmin.



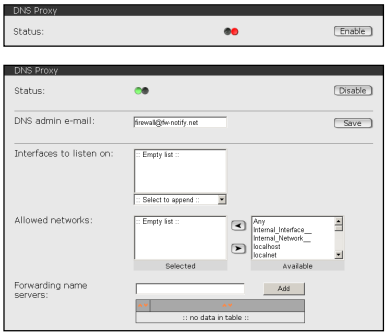
Die Pinne

Falls Sie während der Konfiguration zwischen mehreren Menüs wechseln müssen, haben Sie die Möglichkeit durch einen Klick auf die entsprechende Pinne dieses Verzeichnis geöffnet zu halten. Das Verzeichnis bleibt geöffnet, wenn die Nadel der Pinne nach unten zeigt.

4.3. Menü

Für jede Funktion des Internet-Sicherheitssystems ist im Konfigurationstool **WebAdmin** ein separates Menü enthalten. Diese Menüs enthalten hilfreiche Werkzeuge, die in diesem Kapitel erklärt werden.

4.3.1. Die Statusampel



Einige Funktionen des Internet-Sicherheitssystems sind nach der Installation per Default-Einstellung ausgeschaltet, da diese zuerst konfiguriert werden müssen. Der aktuelle Status einer Funktion wird durch die Statusampel angezeigt:

rot = Funktion ist ausgeschaltet

grün = Funktion ist eingeschaltet

Die Werkzeuge zur Konfiguration dieser Funktionen und Dienste werden erst geöffnet, wenn die Statusampel Grün zeigt.

4.3.2. Die Auswahlfelder

Zur Konfiguration des Systems stehen zwei Varianten dieser Auswahlfelder zur Verfügung.

Mit **Auswahlfeld A** werden den Funktionen und Diensten die dafür **befugten Netzwerke** (Allowed Networks) und **Benutzer** (Allowed Users) zugeordnet.

Netzwerk oder Benutzer zuordnen:

1. Wählen Sie im Feld **Available** das Netzwerk bzw. den Benutzer aus, indem Sie den entsprechenden Namen mit der Maus markieren.

   Sie können mehrere Namen auf einmal auswählen, indem Sie die **Shift**-Taste während der Auswahl gedrückt halten.

2. Klicken Sie auf die Schaltfläche **Pfeil nach links**.

   Der Name wird nun in das Feld **Selected** verschoben.

Netzwerk oder Benutzer entnehmen:

1. Wählen Sie im Feld **Selected** das Netzwerk bzw. den Benutzer aus, indem Sie den entsprechenden Namen mit der Maus markieren.

   Sie können mehrere Namen auf einmal auswählen, indem Sie die **Shift**-Taste während dem Markieren gedrückt halten.

2. Klicken Sie auf die Schaltfläche **Pfeil nach rechts**.

   Der Name wird nun in das Feld **Available** verschoben.

Mit **Auswahlfeld B** wird den Funktionen und Diensten die entsprechende **Authentifizierungsmethode** oder eine **Netzwerkkarte** (Interface) zugewiesen.

Die Authentifizierungsmethode und die Netzwerkkarten müssen vom Administrator zuerst konfiguriert werden. Falls entsprechende Definitionen zur Verfügung stehen, wird die Meldung **Select to append** angezeigt. Falls dem Auswahlfeld keine Definitionen zur Verfügung stehen, erscheint die Meldung **Empty List**.

Authentifizierungsmethode oder Netzwerkkarte zuordnen:

1. Öffnen Sie das Drop-down-Menü.

2. Wählen Sie die Authentifizierungsmethode bzw. die Netzwerkkarte aus, indem Sie mit der Maus auf den entsprechenden Namen klicken.

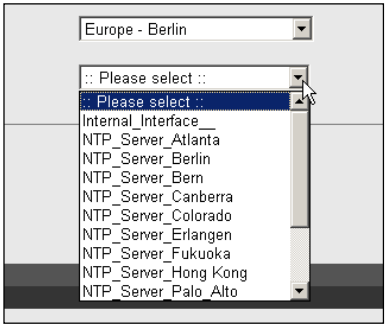
   Der Name wird sofort in das Feld verschoben.

Authentifizierungsmethode oder Netzwerkkarte entnehmen:

1. Markieren Sie im Auswahlfeld den Namen, der aus der Zuordnung gelöscht werden soll durch einen Doppelklick.

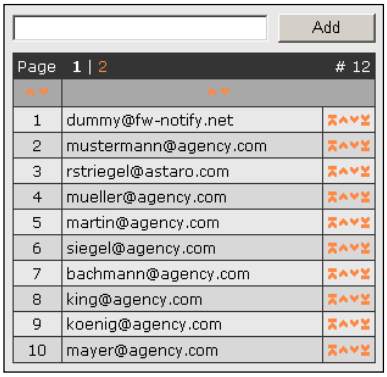
   Der Name wird sofort in das Drop-Down-Menü verschoben.

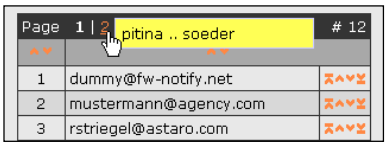
4.3.3. Das Drop-down-Menü



Das **Drop-down-Menü** wird bei Funktionen verwendet, für die immer nur ein bestimmter Wert eingestellt werden kann.
Bei den Drop-down-Menüs werden die ausgewählten Werte in der Regel sofort vom System übernommen.

4.3.4. Das Hierarchiefeld





Das **Hierarchiefeld** kommt bei Funktionen zum Einsatz, bei denen mehrere E-Mail- oder IP-Adressen zugewiesen werden können. Im Hierarchiefeld werden pro Seite 10 Einträge dargestellt.

Im Menü **Interfaces** wird das Hierarchiefeld als **Zugriffskontrollliste** zur Konfiguration des Schnittstellen-Typs **Wireless LAN Access Point** eingesetzt.

In der ersten Zeile wird die Anzahl der Seiten (Page) und der Einträge (#) angezeigt. Die aktuelle Seitenzahl ist weiß dargestellt. Wenn Sie mit der Maus die roten Seitenzahlen berühren, werden in einer Info-Box die darin ent-

haltenen Intervalle angezeigt (kleines Bild). Mit den Pfeilen in der zweiten Zeile kann die Reihenfolge der Einträge verändert werden. Die hier durchgeführten Einstellungen haben allerdings keinen Einfluss auf die Funktionalität:

Mit den Schaltflächen ^ und v in der linken Spalte werden die Einträge in der Tabelle numerisch auf- bzw. absteigend dargestellt. Mit den Schaltflächen ^ und v in der mittleren Spalte werden die Einträge alphanumerisch auf- bzw. absteigend dargestellt.

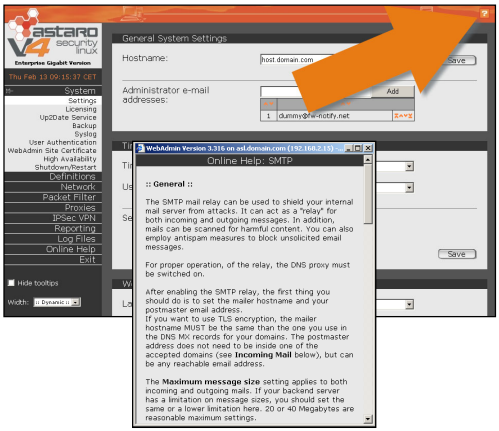
Die funktionale Reihenfolge der Einträge wird mit den Schaltflächen in der rechten Spalte verändert. Durch einen Klick auf die Schaltflächen ^ oder v wird der jeweilige Eintrag um eine Zeile nach vorne bzw. nach hinten verschoben.
Durch einen Klick auf die Schaltfläche ⤒ oder ⤓ wird der jeweilige Eintrag in die erste bzw. in die letzte Zeile der Tabelle verschoben.

Eintrag hinzufügen: Schreiben Sie die neue Adresse in das Eingabefeld und klicken Sie auf die Schaltfläche **Add**.
Die neue Adresse wird anschließend in die letzte Zeile der Tabelle eingefügt.

Eintrag löschen: Durch einen Doppelklick auf die entsprechende Adresse wird diese sofort aus der Tabelle gelöscht.

Eintrag bearbeiten: Durch einen Klick auf die entsprechende Adresse, wird diese in das Eingabefeld geladen. Der Eintrag kann nun im Eingabefeld bearbeitet werden.
Durch einen Klick auf die Schaltfläche **Replace** wird der alte Eintrag ersetzt.

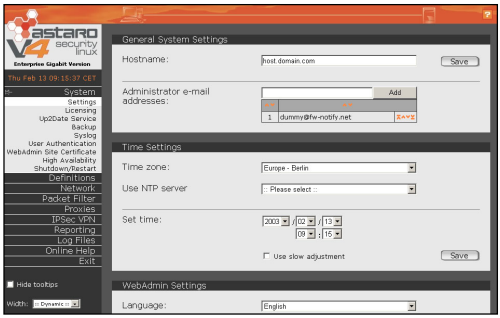
4.4. Online-Hilfe


General System Settings
Hostname:
Administrator e-mail addresses:
Online Help: SMTP
:: General ::
The SMTP mail relay can be used to shield your internal mail server from attacks. It can act as a "relay" for both incoming and outgoing messages. In addition, mails can be scanned for harmful content. You can also employ antispam measures to block unsolicited email messages.
For proper operation, of the relay, the DNS proxy must be switched on.
After enabling the SMTP relay, the first thing you should do is to set the mailer hostname and your postmaster email address.
If you want to use TLS encryption, the mailer hostname MUST be the same than the one you use in the DNS MX records for your domains. The postmaster address does not need to be inside one of the accepted domains (see Incoming Mail below), but can be any reachable email address.
The Maximum message size setting applies to both incoming and outgoing mails. If your backend server has a limitation on message sizes, you should set the same or a lower limitation here. 20 or 40 Megabytes are reasonable maximum settings.

Jedes Menü im Konfigurationstool **WebAdmin** enthält eine **Online-Hilfe** (Online Help), in der die Funktionen kurz erläutert werden. Die Hilfe ist zur Zeit nur in englischer Sprache verfügbar.

Die Hilfe wird durch einen Klick auf die Schaltfläche **?** geöffnet.

5. System bedienen & beobachten



WebAdmin ist das web-basierte Konfigurationstool, das Sie bereits von der Installation her kennen.
In diesem Kapitel werden ausführlich die Bedienung des Sicherheitssystems und seine Funktionen beschrieben. Die verschiedenen Einstellungen werden anhand von Step-by-step-Anleitungen erläutert. Dabei wird allerdings nicht auf die Funktionsweise der Werkzeuge eingegangen. Die Werkzeuge werden in Kapitel 4 beschrieben.

Das Ziel des Administrators sollte sein, so wenig wie möglich und so viel wie nötig durch das Sicherheitssystem zu lassen. Dies gilt sowohl für eingehende als auch für ausgehende Verbindungen.

Tipp:

Planen Sie zuerst Ihr Netzwerk und überlegen Sie sich genau welchen Rechnern welche **Dienste (Services)** zugeordnet werden sollen. Dies vereinfacht Ihnen die Konfiguration und erspart Ihnen viel Zeit, die Sie sonst für die nachträgliche Definition von Netzwerken oder Diensten benötigen.

Gehen Sie bei der Konfiguration des Internet-Sicherheitssystems und Ihres Netzwerks folgendermaßen vor:

1. Richten Sie alle erforderlichen Netzwerke und Hosts ein.
2. Definieren Sie die benötigten Dienste auf dem Internet-Sicherheitssystem.
3. Führen Sie nun die Definition Ihres Gesamtsystems durch.

WebAdmin starten:

1. Starten Sie Ihren Browser und geben die IP-Adresse des Internet-Sicherheitssystems (eth0) wie folgt ein: https://IP-Adresse.
   (Beispiel aus Kapitel 3.2 Installationsanleitung, Schritt 6: https://192.168.2.100)

   Falls Sie noch kein **CA-Zertifikat** für Ihre **WebAdmin**-Seite generiert haben, erscheint ein **Sicherheitshinweis**.
   Ausführliche Informationen zum Zertifikat und wie Sie dieses installieren, finden Sie in Kapitel 5.1.7 ab Seite 86.

2. Bestätigen Sie die Frage auf dem Sicherheitshinweis, ob der Vorgang fortgesetzt werden soll, mit einem Klick auf die Schaltfläche **Ja**.

3. Authentifizieren Sie sich im **WebAdmin**.

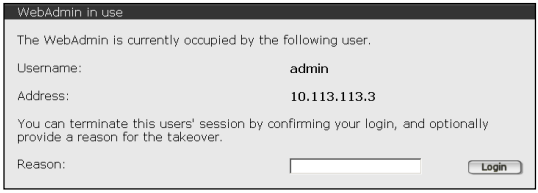
User: **admin**

Password: Passwort des WebAdmin-Benutzers

   Beachten Sie bitte die Groß- und Kleinschreibung!

4. Klicken Sie auf die Schaltfläche **Login**.

   Ein anderer Administrator ist schon eingeloggt:


WebAdmin in use
The WebAdmin is currently occupied by the following user.
Username:
admin
Address:
10.113.113.3
You can terminate this users' session by confirming your login, and optionally provide a reason for the takeover.
Reason:
Login

Sollte bereits ein anderer Administrator im Konfigurationstool **WebAdmin** angemeldet sein, wird eine entsprechende Meldung angezeigt. Anhand der IP-Adresse können Sie sehen, von welchem Rechner auf das Internet-Sicherheitssystems zugegriffen wird.

Sie können diese Session beenden!

Geben Sie im Eingabefeld **Reason** den Grund für die Übernahme an und klicken anschließend auf die Schaltfläche **Login**.

Nun sind Sie im Internet-Sicherheitssystem eingeloggt und können über das Konfigurationstool **WebAdmin** das System bedienen und beobachten.

5.1. Grundeinstellungen (System)

Im Verzeichnis **System** führen Sie die Grundeinstellungen des Internet-Sicherheitssystems durch.

5.1.1. Settings

General System Settings

Hostname: Tragen Sie in das Eingabenfeld den Hostnamen (z. B. FIREWALL.meinedomain.com) ein und speichern Sie Ihre Eingabe durch einen Klick auf die Schaltfläche **Save**.

Hinweis:

In allen **Notification E-Mails** an den Administrator wird in der Betreffzeile der **Hostname** angezeigt.

Administrator e-mail addresses: Bei wichtigen Ereignissen, z. B. auftretenden Portscans, Anmeldungen mit falschem Passwort, Meldungen des Selfmonitors, bei Up2Date-Prozessen oder bei einem Neustart, werden die Administratoren über die im Hierarchiefeld eingetragenen Adressen benachrichtigt. Es sollte mindestens eine E-Mail-Adresse eingetragen sein. Falls keine Adresse im Hierarchiefeld eingetragen ist, wird das komplette Modul **Reporting per E-Mail** ausgeschaltet.
Neue E-Mail-Adressen werden vom Eingabefeld durch einen Klick auf die Schaltfläche **Add** in das Hierarchiefeld übernommen.

Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Wichtiger Hinweis:

An die E-Mail-Adresse des Administrators können **Notification E-Mails** nur zugestellt werden, wenn zuvor der DNS-Proxy (Kapitel 5.5.2 ab Seite 183) eingeschaltet und konfiguriert wurde oder wenn im Menü **SMTP** (Kapitel 5.5.6 ab Seite 190) die Route für eingehende E-Mails definiert wurde.

Use external indicators: Dieser Schalter wird nur angzeigt, wenn das Internet-Sicherheitssystem auf einer Appliance mit LCD-Anzeige läuft. Mit diesem Schalter können Sie die LCD-Anzeige ein- und ausschalten.

Time Settings

Über dieses Menü stellen Sie das aktuelle Datum und die Uhrzeit des Internet-Sicherheitssystems ein. Sie können die Uhrzeit und das Datum mit Hilfe der Drop-down-Menüs manuell einstellen oder täglich mit einem NTP-Server (Network Time Protocol) synchronisieren. Beachten Sie, dass große Zeitsprünge zu Lücken im **Reporting** und im **Logging** führen.

Wichtiger Hinweis:

Führen Sie keine Umstellung von Winterzeit auf Sommerzeit durch. Tragen Sie am Besten die Central European Time (CET) ein. Während der Sommerzeit entspricht dies einer Abweichung von minus einer Stunde.

Durch Verstellen der Systemzeit kann es zu folgenden Time Warp-Effekten kommen:

Uhrzeit vorstellen (Winter- auf Sommerzeit)

- Der Time-out für den **WebAdmin** ist abgelaufen und Ihre Session ist nicht mehr gültig.
- In den zeitbasierten Reports fehlen für die entsprechende Zeitspanne die Log-Daten. Die meisten Diagramme stellen diese Zeitspanne als gerade Linie in Höhe des alten Wertes dar.
- Für das **Accounting** betragen alle Werte in dieser Zeitspanne 0.

Uhrzeit zurückstellen (Sommer- auf Winterzeit)

- In den zeitbasierten Reports gibt es für die entsprechende Zeitspanne schon Log-Daten, die aus Sicht des Systems aber aus der Zukunft kommen: Diese Daten werden nicht überschrieben.
- Die Log-Dateien werden weitergeschrieben, wenn der Zeitpunkt vor dem Zurückstellen wieder erreicht ist.
- Die meisten Diagramme stellen die Werte dieser Zeitspanne zusammengepresst dar.

- Für das **Accounting** behalten die bereits erfassten Daten (aus der Zukunft) ihre Gültigkeit. Die Accounting-Dateien werden weitergeschrieben, wenn der Rückstell-Zeitpunk wieder erreicht ist.

Es wird daher geraten, die Zeit nur bei der Erst-Konfiguration einmalig zu setzen und später nur geringfügig anzupassen. Verwenden Sie am Besten die Central European Time (CET). Dies ist die ursprüngliche Uhrzeit. Das System läuft dann immer in CET, nicht in CEST (Central European Summer Time). Umstellungen von Winter- und Sommerzeit sollten nicht vorgenommen werden, insbesondere wenn die gesammelten Reporting- und Accounting-Daten weiterverarbeitet werden.

Systemzeit manuell einstellen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Settings**.

2. Führen Sie im Fenster **Time Settings** folgende Einstellungen in der angegebenen Reihenfolge durch:

   Use NTP server: Vergewissern Sie sich für die manuelle Zeiteinstellung des Internet-Sicherheitssystems, dass hier kein NTP-Server ausgewählt ist. Sollte dies nicht der Fall sein, wählen Sie im Drop-down-Menü **No NTP Server** aus.

   Time zone: Wählen Sie nun die Zeitzone aus.

   Hinweis:

   Die neu definierte Zeitzone hat nur eine Auswirkung auf die derzeit eingestellte Uhrzeit, wenn Sie bereits einen NTP-Server eingerichtet haben.

   Use slow adjustment: Durch diese Option werden mögliche Time Warp-Effekte, wie sie in der Einleitung beschrieben sind, ausgeglichen.

   Hinweis:

   Beim Zurückstellen erfolgt das Heranführen der Systemzeit an die neu eingestellte Uhrzeit in kleinen Schritten. Dies kann dann bei großen Zeitintervallen Tage oder sogar Wochen dauern.

   Set time: Stellen Sie das Datum und die Uhrzeit ein.

Wichtiger Hinweis:

Beachten Sie bei der Eingabe des aktuellen Datums das Ausgabedatum des License-Key. Falls das Ausgabedatum des Keys nach dem aktuellen Datum liegt, wird die Lizenz deaktiviert. Es wird nicht automatisch die Evaluation License (30-Tage-Testlizenz) aktiviert.

3. Speichern Sie Ihre Einstellungen durch einen Klick auf die Schaltfläche **Save**.

Die Uhrzeit des Systems wird nun aktualisiert.

Hinweis:

Falls Sie die Option **Use slow adjustment** aktiviert haben, wird der Haken aus dem Optionsfeld gelöscht und die alte Systemuhrzeit (**System time**) wird weiterhin angezeigt. Die Anzeige wird aktualisiert, sobald der Vorgang beendet ist.

Systemzeit mit NTP-Server synchronisieren:

Bevor die Uhrzeit des Internet-Sicherheitssystems mit einem externen System synchronisiert werden kann, muss dieses als **NTP-Server** definiert werden. Der **NTP-Server** wird dabei als Netzwerk bestehend aus einem Rechner definiert. Verschiedene öffentliche NTP-Server sind bereits vordefiniert.

Das Definieren von Netzwerken wird ausführlich in Kapitel 5.2 ab Seite 96 beschrieben. Wenn der NTP-Server bereits definiert ist, oder Sie einen der vordefinierten Server verwenden möchten, beginnen Sie mit Schritt 6.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen**.
   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

3. Tragen Sie nun die **IP-Adresse** des **NTP-Servers** ein.

4. Im Eingabefeld **Subnet mask** geben Sie die **Netzwerkmaske** 255.255.255.255 ein.

5. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   WebAdmin prüft nun Ihre Eingaben auf semantische Gültigkeit. Nach erfolgreicher Definition wird das neue Netzwerk in die Netzwerk-Tabelle eingetragen.

6. Öffnen Sie im Verzeichnis **System** das Menü **Settings**.

7. Führen Sie im Fenster **Time Settings** folgende Einstellungen in der angegebenen Reihenfolge durch:

   Time zone: Wählen Sie zuerst die Zeitzone aus.

   Use NTP server: Wählen Sie hier den NTP-Server aus.

Die Uhrzeit des Internet-Sicherheitssystems wird nun mit dem externen System jede volle Stunde synchronisiert.

WebAdmin Settings

In diesem Menü richten Sie den Zugang zum Konfigurationstool **WebAdmin** ein.

Automatisch schließen, Dauer einstellen:

Im Eingabefeld **Timeout (seconds)** geben Sie die Zeitspanne in Sekunden an, in der Sie vom **WebAdmin** automatisch ausgeloggt werden, wenn keine Aktionen stattfinden. Nach der Installation sind standardmäßig 300 Sekunden eingestellt. Die kleinstmögliche Zeitspanne beträgt 60 Sekunden.
Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

Wenn sie den Browser mit einer offenen **WebAdmin**-Session schließen ohne den **WebAdmin** über **Exit** zu verlassen, bleibt die letzte Session bis zum Ablauf des Time-outs aktiv.

WebAdmin TCP Port ändern:

Falls Sie den Standard-Port 443 für den HTTPS-Dienst anderweitig verwenden wollen (z. B. eine Umleitung mit **DNAT**), müssen Sie hier einen anderen TCP Port für das **WebAdmin** Interface angeben. Mögliche Werte sind 1024-65535, wobei

bestimmte Ports für andere Dienste reserviert sind. Um den **WebAdmin** nach einer Änderung anzusprechen, müssen Sie den Port mit einem Doppelpunkt getrennt an die Sicherheitssystem-IP-Adresse anhängen, z. B.: https://192.168.0.1:1443.

Im Auswahlfeld **Allowed networks** werden die Netzwerke hinzugefügt, von denen aus auf **WebAdmin** zugegriffen werden darf. Wie auch bei **SSH** ist hier für eine reibungslose Installation **Any** eingetragen. In diesem Fall darf, falls das Passwort zur Verfügung steht, von überall auf **WebAdmin** zugegriffen werden.

Sicherheitshinweis:

Sobald Sie einschränken können, von wo aus das Internet-Sicherheitssystem administriert werden soll (z. B. Ihre IP-Adresse im lokalen Netzwerk), ersetzen Sie den Eintrag **Any** im Auswahlfeld **Allowed networks** durch ein kleineres Netzwerk.

Am sichersten ist es, wenn nur ein Administrations-PC per HTTPS auf das Internet-Sicherheitssystem Zugriff hat.
Netzwerke definieren Sie im Menü **Definitions/Networks**.

Mit dem Auswahlfeld **Authentication methods** bestimmen Sie die Methode zur Authentifizierung. Damit Sie nach der Installation über das Konfigurationstool **WebAdmin** Zugriff auf das Internet-Sicherheitssystem haben, wurde hier bereits während der Installation die Authentifizierungsmethode **Local Users** definiert und im Auswahlmenü **Allowed Users** der entsprechende **Benutzer (User)** angelegt.

Weitere mögliche Authentifizierungsmethoden sind **NT/2000/ XP Server**, **RADIUS Database** und **LDAP Server**.

Die lokalen **Benutzer (Users)** werden im Menü **Definitions/ Users** verwaltet.

SSH (Shell Access) Settings

Die **Secure Shell (SSH)** ist eine textorientierte Schnittstelle zum Internet-Sicherheitssystem, die allerdings nur für erfahrene Administratoren geeignet ist. Man benötigt für den Zugriff per **SSH** einen **SSH-Client**, der in den meisten Linux-Distributionen bereits vorhanden ist. Unter MS Windows ist das Programm **Putty** als **SSH-Client** zu empfehlen. Der Zugriff per **SSH** ist verschlüsselt und somit für Fremde nicht mitzulesen.

Die Funktion Shell Access ist per Default eingeschaltet, wenn Sie im Fenster **Setting System Passwords** für die Konfiguration über den **Astaro Configuration Manager** ein Passwort gesetzt haben.

Wenn Sie über **SSH** auf das Internet-Sicherheitssystem zugreifen wollen, muss der SSH-Status eingeschaltet sein (Statusampel zeigt Grün).
SSH benötigt für die Protokollierung des Zugriffs **Namensauflösung** (gültige Nameserver), anderenfalls gibt es bei der SSH-Anmeldung einen Time-out. Dieser Time-out dauert etwa eine Minute an. In dieser Zeit sieht es so aus, als wäre die Verbindung eingefroren oder würde nicht zustande kommen. Danach geht es ohne Verzögerung weiter.

Zusätzlich müssen Sie im Auswahlfeld **Allowed networks** die Netzwerke hinzufügen, von denen aus per **SSH** auf das Internet-Sicherheitssystem zugegriffen werden soll.
Per Default-Einstellung ist im Auswahlfeld **Allowed networks** für eine reibungslose Installation die Option **Any** eingetragen, d. h. jeder ist berechtigt auf den SSH-Dienst zuzugreifen.
Netzwerke definieren Sie im Menü **Definitions/Networks**.

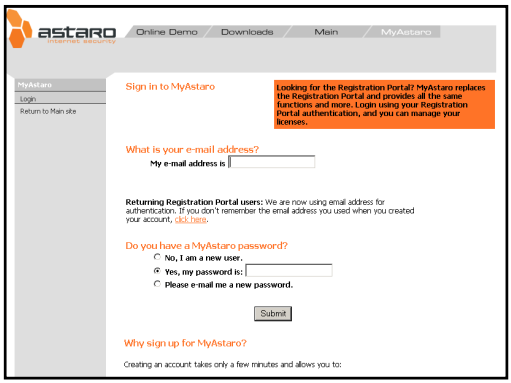
Sicherheitshinweis:

Per Default-Einstellung ist jeder berechtigt auf den SSH-Dienst zuzugreifen. Im Auswahlfeld **Allowed networks** ist die Option **Any** eingetragen. Aus Sicherheitsgründen empfehlen wir den Zugriff auf den SSH-Dienst zu beschränken. Alle anderen Netzwerke sollten sie löschen!

Schalten Sie aus Sicherheitsgründen den **SSH**-Zugang nach Abschluss der Arbeiten wieder ab.

5.1.2. Licensing

Einige Funktionen dieses Internet-Sicherheitssystems, z. B. der **Up2Date Service**, **High Availability (HA)**, **Surf Protection** und **Virus Protection** sowie das **Support**-Angebot des Astaro-Partners können nur mit einem entsprechend gültigen License-Key in Anspruch genommen werden. Ausführliche Informationen zur Lizensierung sowie den entsprechenden License-Keys erhalten Sie bei einem zertifizierten Astaro-Partner oder Sie wenden sich über die E-Mail-Adresse **sales@astaro.com** direkt an Astaro.


astaro
Online Demo
Downloads
Main
MyAstaro
MyAstaro
Login
Return to Main site
Sign in to MyAstaro
Looking for the Registration Portal? MyAstaro replaces the Registration Portal and provides all the same functions and more. Login using your Registration Portal authentication, and you can manage your licenses.
What is your e-mail address?
My e-mail address is
Returning Registration Portal users: We are now using email address for authentication. If you don't remember the email address you used when you created your account, click here.
Do you have a MyAstaro password?
No, I am a new user.
Yes, my password is:
Please e-mail me a new password.
Submit
Why sign up for MyAstaro?
Creating an account takes only a few minutes and allows you to:

Ab **Astaro Security Linux Version 3** benötigen Sie zuerst den Activation-Key. Mit diesem Activation-Key aktivieren Sie in **MyAstaro** den License-Key. Auf diese Weise können Sie selbst den Beginn des Lizenzzeitraums des Internet-Sicherheitssystems bestimmen. Sie können also zuerst die Software installieren und registrieren anschließend im Registrierungs-Portal Ihre Lizenz – erst ab diesem Zeitpunkt läuft die Zeitspanne für die erworbenen Optionen.

Hinweis:

Die neuen Activation-Keys können nicht direkt über das Konfigurationstool **WebAdmin** eingespielt werden. Sie müssen erst auf **MyAstaro** registriert werden.

Benutzer-Account festlegen:

1. Öffnen Sie mit Ihrem Browser die Internetseite mit der Adresse https://my.astaro.com.

2. Melden Sie sich in **MyAstaro** an.

   What is your e-mail address?

   Für die Authentifizierung wird die E-Mail-Adresse verwendet. Als Neukunde tragen Sie hier Ihre E-Mail-Adresse ein.

   Wenn Sie bereits das **Registration Portal** genutzt haben, tragen Sie in das Eingabefeld die E-Mail-Adresse ein, die Sie bei der Anmeldung verwendet haben. Falls Sie die damals verwendete E-Mail-Adresse nicht mehr wissen, können Sie diese unter dem Dialog **Returning Registration Portal users** abfragen. Sie benötigen Ihr **Username** und das **Password**.

   Do you have a MyAstaro password?

   Falls Sie sich zum ersten Mal in *MyAstaro* anmelden, klicken Sie das Auswahlkästchen bei **No, I am a new user** an. Falls Sie bereits Benutzer von MyAstaro sind, tragen Sie das Passwort in das Eingabefeld **Yes, my password is** ein.

   Klicken Sie anschließend auf die Schaltfläche **Submit**.

3. Generieren Sie einen **MyAstaro Accout**.

   E-Mail Address: In diesem Eingabefeld können Sie Ihre Adresse korrigieren.

   Password: Tragen Sie Ihr gewünschtes Passwort ein.

   First Name: Tragen Sie Ihren Vornamen ein.

   Last Name: Tragen Sie Ihren Nachnamen ein.

   Klicken Sie anschließend auf die Schaltfläche **Register**.

   Bei erfolgreicher Registrierung wird nun die Seite mit der Meldung **Congratulations, you have created your**

MyAstaro account. Des Weiteren wird Ihnen per E-Mail eine Bestätigung zugesendet.

Sie können nun in **MyAstaro** verschiedene Versionen des Internet-Sicherheitssystems herunterladen und zu Ihrer Lizenz die folgenden Aktionen durchführen:

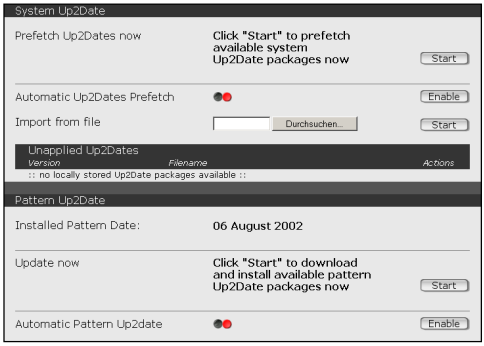
1. V4-Lizenzen zu Version 5-Lizenzen konvertieren
2. gekaufte Version-4-Activation-Keys registrieren
3. Optionen zu registrierten Lizenzen hinzufügen
4. eine kostenlose Home-User-Lizenz herunterladen

Internet-Sicherheitssystem lizenzieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Licensing**.
2. Tragen Sie den License-Key in das Eingabefeld **License Key** ein und klicken Sie anschließend auf die Schaltfläche **Save**.

Die Generierung des Systems dauert ca. 5 bis 10 Sekunden. Nach erfolgreicher Registrierung des Internet-Sicherheitssystems erhalten Sie im Fenster **License Information** Angaben zu Ihrer Lizenz.

5.1.3. Up2Date Service



Mit dem **Up2Date Service** halten Sie Ihr System auf dem neusten Stand: Neue Viren-Pattern, System-Patches und Sicherheits-Features werden in Ihr laufendes System eingespielt.

Die **Up2Date**-Pakete sind signiert und verschlüsselt, und werden zudem über eine verschlüsselte Verbindung eingespielt. Nur Astaro ist berechtigt, solche **Up2Date**-Pakete zu erstellen und zu signieren. Nicht korrekt signierte **Up2Date**-Pakete werden als solche erkannt und gelöscht.

Für **System Up2Date** und für **Pattern Up2Date** gibt es mehrere Up2Date-Server, die der Reihe nach angewählt werden. Falls ein Up2Date-Server nicht erreichbar ist, wird der nächste Server nach System- bzw. Pattern Up2Dates abgefragt.

Wichtiger Hinweis:

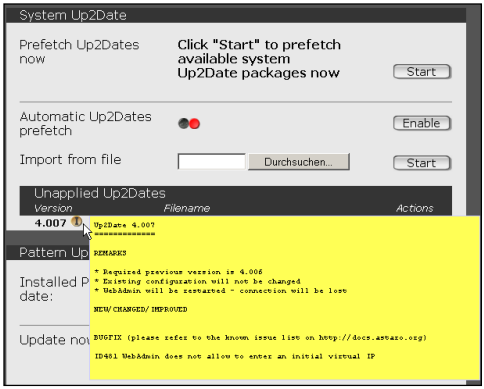
Der **Up2Date Service** benutzt eine TCP-Verbindung auf Zielport 222, um die Up2Date-Pakete herunterzuladen. Das Internet-Sicherheitssystem selbst erlaubt diese Verbindung ohne weitere Einstellungen. Falls Sie jedoch eine übergeordnete (Upstream) Firewall verwenden, müssen Sie auf dieser die Kommunikation über Port 222 TCP zu den Update-Servern erlauben.

Hinweis:

Beachten Sie beim **High Availability (HA)**-System die gesonderte Funktionsweise des **System Up2Date**.

System Up2Date

Mit der Funktion **System Up2Date** importieren Sie System-Patches und neue Sicherheits-Features auf Ihr Internet-Sicherheitssystem. Die **Up2Date**-Pakete können über eine verschlüsselte Verbindung manuell oder automatisch vom Update-Server heruntergeladen werden. Falls Sie nicht über eine Internetverbindung verfügen, können die Up2Date-Pakete von einem lokalen Datenträger aus eingespielt werden.



Neu eingespielte Up2Date-Pakete werden in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Diese Up2Date-Pakete sind noch nicht installiert!
Weitere Informationen erhalten Sie, wenn Sie mit dem Cursor die **gelbe Info-Schaltfläche** berühren. Falls die Info-Schaltfläche in **rot** angezeigt wird, wird nach der Installation des Up2Date-Pakets automatisch ein **Restart** des Sicherheitssystems durchgeführt.

Hinweis:

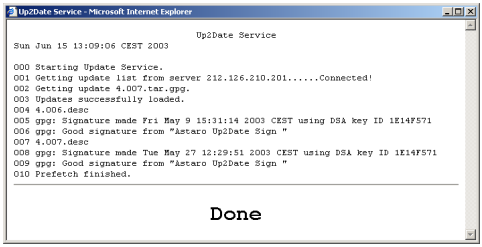
Beachten Sie beim **High Availability (HA)**-System die zusätzlichen Hinweise zum Einspielen und Installieren der **System Up2Dates**.
Das **HA**-System wird in Kapitel 5.1.8 ab Seite 89 erklärt.

Fehlende Up2Date-Pakete können Sie unter der Internetadresse **http://download.astaro.de/ASL/up2date** auf Ihren lokalen Rechner herunterladen.

System Up2Date manuell einspielen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Klicken Sie im Fenster **System Up2Date** auf die Schaltfläche **Start** bei **Prefetch Up2Dates now**.


Up2Date Service - Microsoft Internet Explorer
Up2Date Service
Sun Jun 15 13:09:06 CEST 2003
000 Starting Update Service.
001 Getting update list from server 212.126.210.201.....Connected!
002 Getting update 4.007.tar.gpg.
003 Updates successfully loaded.
004 4.006.desc
005 gpg: Signature made Fri May 9 15:31:14 2003 CEST using DSA key ID 1E14F571
006 gpg: Good signature from "Astaro Up2Date Sign "
007 4.007.desc
008 gpg: Signature made Tue May 27 12:29:51 2003 CEST using DSA key ID 1E14F571
009 gpg: Good signature from "Astaro Up2Date Sign "
010 Prefetch finished.
Done

Das System prüft nun, ob auf dem Update-Server neue Up2-Date-Pakete vorhanden sind und lädt diese herunter. Der gesamte Up2Date-Vorgang wird im **Log-Fenster** in Echtzeit dargestellt (linkes Bild). Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

Die in der Tabelle **Unapplied Up2Dates** aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

System Up2Date über Internet automatisch einspielen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Automatic Up2Dates Prefetch** ein.

3. Definieren Sie im Auswahlfeld **Interval** den Zeitabstand, nach dem das System automatisch den spezifizierten **Update-Server** anwählt und diesen auf neue **System Up2Dates** überprüft.

   Die möglichen Zeitintervalle sind: Jede Stunde, jeden Tag, einmal pro Woche.

Neu eingespielte Up2Date-Pakete werden in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Weitere Informationen erhalten Sie mit Hilfe der Info-Schaltfläche.
Die in der Tabelle aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

System Up2Date von lokalem Datenträger einspielen:

Der Dateiname eines Up2Date-Pakets setzt sich aus der Versionsnummer, der Bezeichnung **tar** für ein verschlüsseltes Archiv und dem Dateitype **.gpg** zusammen. Beispiel: 3.033.tar.gpg. Up2Date-Pakete finden Sie auf dem FTP-Server **ftp.astaro.com**.

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Klicken Sie im Fenster **System Up2Date** auf die Schaltfläche **Durchsuchen** bei **Import from file**.

3. Wählen Sie im Fenster **Datei auswählen** das Up2Date-Paket aus, das Sie importieren möchten und klicken auf die Schaltfläche **Öffnen**.

Wichtiger Hinweis:

Verwenden Sie zum Importieren der Up2Date-Pakete unter Microsoft Windows keinen **UNC-Pfad**. Wählen Sie die Pakete mit Hilfe des Auswahlfeldes **Durchsuchen** aus.

4. Klicken Sie im Fenster **System Up2Date** bei **Import from file** auf die Schaltfläche **Start**.

   Neu eingespielte Up2Date-Pakete werden anschließend in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Weitere Informationen erhalten Sie mit Hilfe der Info-Schaltfläche.
   Die in der Tabelle aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

5. Wiederholen Sie nun die Schritte 2 bis 4 bis Sie alle Up2Date-Pakete importiert haben.

System Up2Date installieren (ohne HA-System):

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Wählen Sie in der Tabelle **Unapplied Up2Dates** das Up2Date-Paket aus.

Hinweis:

Falls die Tabelle mehr als ein **System Up2Date**-Paket enthält, starten Sie die Installation mit der **aktuellsten** Version. Die älteren Versionen werden dann automatisch installiert.

3. Klicken Sie nun in der Spalte **Actions** auf **Install**.

   Die Installation der Up2Date-Pakete wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

System Up2Date auf HA-Lösung installieren:

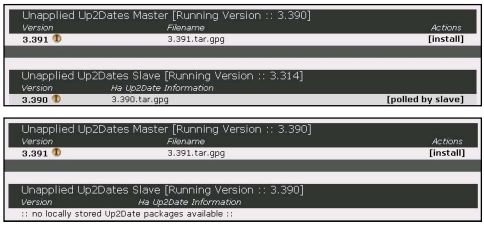
1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Wählen Sie in der Tabelle **Unapplied Up2Dates Master** das Up2Date-Paket aus.

Hinweis:

Falls die Tabelle mehr als ein **System Up2Date**-Paket enthält, starten Sie die Installation mit der **kleinsten** Version. Auf dem **HA**-System kann immer nur ein Paket installiert werden.

3. Klicken Sie nun in der Spalte **Actions** auf **Install**.

   Die Installation des Up2Date-Pakets auf dem System 1 wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.



   Anschließend wird die Installation automatisch auf dem System 2 gestartet. In der Tabelle **Unapplied Up2Dates Slave** wird während des Vorgangs das Up2Date-Paket und die Meldung **Polled by slave** angezeigt.

   Die Installation auf dem System 2 wurde erfolgreich beendet, wenn in der Tabelle wieder die Meldung **No locally stored Up2Date packages available** erscheint.

4. Falls in der Tabelle **Unapplied Up2Dates Master** noch Up2Date-Pakete angezeigt werden, wiederholen Sie die Schritte 2 und 3 solange bis keine Up2Date-Pakete mehr verfügbar sind.

   Auf dem **HA**-System wurden alle verfügbaren Up2Date-Pakete installiert, wenn in der Tabelle **Unapplied Up2Dates Master** die Meldung **No locally stored Up2Date packages available** erscheint und die angezeigten Versionen der beiden Systeme übereinstimmen.

Pattern Up2Date

Mit der Funktion **Pattern Up2Date** aktualisieren Sie den Virusscanner Ihres Internet-Sicherheitssystems mit neuen Virus-Patterns. Sie haben die Möglichkeit, den Virusscanner manuell oder automatisch in bestimmten Zeitintervallen auf dem neusten Stand zu halten.

Installed Pattern Date informiert Sie, welches **Pattern Up2Date**-Paket zuletzt installiert wurde.

Pattern Up2Date, manuell:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Klicken Sie im Fenster **Pattern Up2Date** auf die Schaltfläche **Start** bei **Update now**.

Das System prüft nun, ob auf dem Update-Server neue Pattern Up2Date-Pakete vorhanden sind, lädt diese herunter und installiert sie auf dem Internet-Sicherheitssystem. Der gesamte Up2Date-Vorgang wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

Die Angabe **Installed Pattern Date** wird sofort aktualisiert, wenn Sie im Verzeichnis **System** auf **Up2Date Service** klicken oder sobald Sie das nächste Mal dieses Menü öffnen.

Bei der **High Availability (HA)**-Lösung wird der Virusscanner von System 2 automatisch mit dem von System 1 synchronisiert.

Pattern Up2Date, automatisch:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Automatic Pattern Up2Date** ein.

3. Definieren Sie im Auswahlfeld **Interval** den Zeitabstand, nach dem das Internet-Sicherheitssystem automatisch den spezifizierten **Up2Date Server** anwählt und diesen auf neue **Pattern Up2Dates** überprüft.

   Die möglichen Zeitintervalle sind: Jede Stunde, jeden Tag, einmal pro Woche.

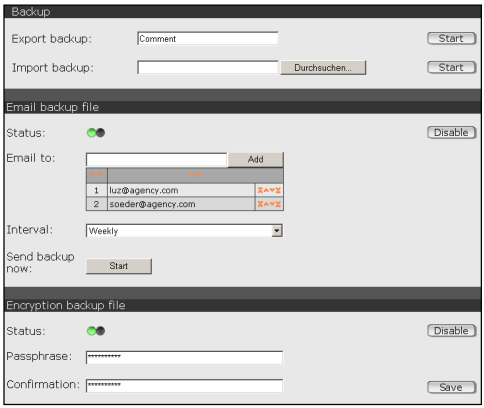
Sicherheitshinweis:

Stellen Sie das Intervall auf jede Stunde ein, damit Ihr Virenscanner immer auf dem aktuellsten Stand ist.

Der automatische **Pattern Up2Date** ist jetzt aktiviert. Das Internet-Sicherheitssystem prüft nun regelmäßig auf dem **Up2Date Server** ob neue **Pattern Up2Dates** zur Verfügung stehen. Sobald ein neues **Pattern Up2Date** installiert ist, erhält der Administrator eine E-Mail, in der die zuletzt installierten Virensignaturen aufgelistet sind.

Beim **High Availability (HA)**-System wird der Virusscanner von System 2 automatisch mit dem von System 1 synchronisiert.

5.1.4. Backup



Mit der **Backup-Funktion** können Sie die Einstellungen Ihres Internet-Sicherheitssystems auf einer lokalen Festplatte sichern.
Mit Hilfe der Backup-Datei sind Sie in der Lage, ein neu installiertes System auf einen identischen Konfigurationsstand zu bringen. Dies ist bei einem Hardwaredefekt besonders hilfreich, da binnen Minuten ein neues Internet-Sicherheitssystem installiert und anschließend das Backup eingespielt werden kann. Bereits nach kurzer Zeit ist auf diese Weise ein Ersatzsystem einsatzbereit.

Achtung:

In die aktuelle System-Version 4.0 kann nur ein Backup aus der Version 3.216 oder höher eingespielt werden.

Falls Sie mehr als drei Netzwerkkarten installiert haben und über eine entsprechende Lizenz verfügen, tragen Sie im Menü **Licensing** zuerst den License-Key ein und spielen anschließend das Backup ein. Vom System werden sonst nur drei Netzwerkkarten hochgefahren und dies kann dazu führen, dass das Konfigurationstool **WebAdmin** nicht mehr erreichbar ist.

Hinweis:

Legen Sie nach jeder Änderung der Systemeinstellungen eine neue Backup-Datei an. Auf diese Weise haben Sie immer die aktuellen Einstellungen Ihres Systems gespeichert. Bewahren Sie dieses Backup an einem sicheren Ort auf, da alle Konfigurations-Einstellungen, z. B. die Zertifikate und Keys, darin enthalten sind.

Prüfen Sie die Backup-Datei nach der Generierung immer auf Lesbarkeit. Es ist außerdem ratsam durch ein externes MD5-Programm eine Prüfsumme zu generieren, die es Ihnen auch später ermöglicht, die Funktionsfähigkeit der Backup-Datei zu prüfen.

Backup manuell generieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.

2. Geben Sie im Fenster **Backup** in das Eingabefeld **Export backup** einen Kommentar ein.
   Wenn Sie später das Backup wieder einspielen, erscheint der Kommentar in der Information.

   Wichtiger Hinweis:

   Falls die Funktion **Encryption Backup File** eingeschaltet ist, wird die Backup-Datei mit **DES** oder **3DES** verschlüsselt und kann später nur mit dem richtigen Passwort wieder eingespielt werden.

3. Um die Backup-Datei zu erzeugen, klicken Sie nun auf die Schaltfläche **Start**.

   Das System generiert nun die Backup-Datei. Wenn die Meldung **Backup has been created successfully** erscheint, wurde der Vorgang erfolgreich abgeschlossen.

4. Um die Backup-Datei auf Ihren lokalen PC zu speichern, klicken Sie nun auf die Schaltfläche **Save**.

5. Wählen Sie in dem Menü **Dateidownload** die Option **Datei auf Datenträger speichern** aus und klicken Sie auf die Schaltfläche **OK**.

6. Im Menü **Datei speichern unter** können Sie die Datei nun unter einem beliebigen Dateinamen speichern.
   Der vom Internet-Sicherheitssystem erzeugte Dateinamen setzt sich aus Backup, Datum und Uhrzeit zusammen:
   backup_yyyymmdd_hhmmss.abf (astaro-backup-file).

Achtung:

Verwenden Sie im Dateinamen nicht die Umlaute Ä, Ö und Ü. Die Datei wird sonst vom Internet-Sicherheitssystem als **corrupt** erkannt und kann nicht eingespielt werden.

7. Prüfen Sie die neu generierte Datei auf Lesbarkeit, indem Sie die Backup-Datei importieren und auf die Schaltfläche **Start** klicken.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.

8. Brechen Sie anschließend den Einspielvorgang ab, indem Sie auf ein Menü im Verzeichnis klicken.

Achtung:

Generieren Sie nach jeder Änderung im System eine neue Backup-Datei. Wenn Sie eine Backup-Datei einspielen und etwa zwischenzeitlich das Passwort oder die IP-Adresse des Internet-Sicherheitssystems geändert haben, kann es passieren dass Sie keinen Zutritt mehr zum System erhalten.

Backup einspielen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.
2. Klicken Sie im Fenster **Backup**, neben dem Eingabefeld **Import backup** auf die Schaltfläche **Durchsuchen**.
3. Wählen Sie im Fenster **Datei auswählen** die Backup-Datei aus, die Sie importieren möchten und klicken auf die Schaltfläche **Öffnen**.

Hinweis:

Verwenden Sie zum Einspielen des Backups unter Microsoft Windows keinen **UNC-Pfad**. Wählen Sie die Backup-Datei mit Hilfe des Auswahlmenüs **Suchen in** aus.

4. Klicken Sie bei **Import backup** auf die Schaltfläche **Start**.

   Falls während der Generierung der Backup-Datei die Funktion **Encryption Backup File** eingeschaltet war, wird nun das Fenster **Enter Passphrase** geöffnet.
5. Tragen Sie in das Eingabefeld **Passphrase** das Passwort ein.
6. Bestätigen Sie die Eingabe durch einen Klick auf die Schaltfläche **Start**.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.
7. Überprüfen Sie die **Backup Information**.
8. Übernehmen Sie die Backup-Datei in das aktive System durch einen Klick auf die Schaltfläche **Start**.

Wenn die Meldung **Backup has been restored successfully** erscheint, wurde der Vorgang erfolgreich abgeschlossen.

E-Mail Backup File

Damit Sie nicht ständig daran denken müssen die Einstellungen Ihres Internet-Sicherheitssystems manuell auf einem Datenträger zu sichern, können Sie hier die Backup-Datei automatisch erzeugen lassen. Im Anschluss wird die Datei an die angegebene E-Mail-Adresse geschickt. Eine E-Mail-Backup-Datei ist ca. 100 KB groß.

E-Mail Backup File generieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.

2. Schalten Sie im Fenster **E-Mail Backup File** die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Die Funktion **E-Mail-Backup File** ist eingeschaltet, wenn die Statusampel Grün zeigt.

   Wichtiger Hinweis:

   Falls die Funktion **Encryption Backup File** eingeschaltet ist, wird die Backup-Datei mit **DES** oder **3DES** verschlüsselt und kann später nur mit dem richtigen Passwort wieder eingespielt werden.

3. Definieren Sie mit dem Drop-down-Menü **Interval** den Zeitabstand nach dem automatisch eine neue Backup-Datei erstellt werden soll.

   Die möglichen Zeitintervalle sind: Täglich, einmal pro Woche und einmal pro Monat.

4. Tragen Sie in das Eingabefeld **E-Mail to** die Adresse ein, an die die automatisch erstellten Backup-Dateien in regelmäßigen Abständen gesendet werden soll.

5. Durch einen Klick auf die Schaltfläche **Add** neben dem Eingabefeld **E-Mail to** übernehmen Sie die neue Adresse in das Hierarchiefeld.

   Wenn Sie weitere E-Mail-Adressen hinzufügen möchten, wiederholen Sie den Schritt 5.

6. Falls die erste Backup-Datei sofort generiert und abgeschickt werden soll, klicken Sie auf die Schaltfläche **Start** neben **Send backup now**.

7. Prüfen Sie die neu generierten Dateien auf Lesbarkeit, indem Sie die jeweilige Backup-Datei importieren und auf die Schaltfläche **Start** klicken.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.

8. Brechen Sie anschließend den Einspielvorgang ab, indem Sie auf ein Menü im Verzeichnis klicken.

E-Mail-Adressen bearbeiten:

Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Encryption Backup File

Die Backup-Datei enthält alle Konfigurations-Einstellungen sowie die darin enthaltenen Zertifikate und Keys. Mit der Funktion **Encryption Backup File** kann die Datei mit **DES** oder **3DES** verschlüsselt werden.

E-Mail Backup File verschlüsseln:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.

2. Scrollen Sie zum Fenster **Encryption Backup File**

3. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Die Funktion **Encryption Backup file** ist eingeschaltet, wenn die Statusampel Grün zeigt.

4. Tragen Sie in das Eingabefeld **Passphrase** das Passwort ein.

Sicherheitshinweis:

Bei einem Passwort mit bis zu sieben Zeichen wird die Backup-Datei mit **DES** verschlüsselt, ab acht Zeichen mit **3DES**.

5. Tragen Sie das Passwort zur Bestätigung nochmals in das Eingabefeld **Confirmation** ein.

6. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

Alle Backup-Dateien, die nun von Ihnen manuell oder vom System automatisch generiert werden, sind mit dem definierten Passwort verschlüsselt.

Wichtiger Hinweis:

Eine mit **Encryption Backup File** verschlüsselte Backup-Datei kann nur mit dem Passwort wieder auf dem System eingespielt werden, das zum Zeitpunkt der Backup-Generierung verwendet wurde.

5.1.5. Syslog

Mit dieser Funktion können Sie die Log-Meldungen des Internet-Sicherheitssystems an verschiedene Hosts weiterleiten. Dies ist besonders dann sinnvoll, wenn Sie die Log-Dateien verschiedener Systeme auf einzelne Hosts zusammenführen wollen.

Achtung:

Wählen Sie im Menü **System/Syslog** als Zieladresse (Host) kein Interface des Internet-Sicherheitssystems, z. B. eth0 aus.

Per Default ist die Funktion ausgeschaltet. Um sie zu aktivieren, wählen Sie im Fenster **Remote Syslog** einen Host aus, der die entsprechende Log-Daten empfangen soll. Nach Auswahl eines Hosts wird die Weiterleitung der entsprechenden Log-Daten ohne eine weitere Meldung gestartet.
Die dazu nötige Definition des Hosts (Netzwerk mit Netzmaske 255.255.255.255) nehmen Sie im Menü **Definitions/Networks** vor. Das Definieren von Netzwerken wird ausführlich in Kapitel 5.2 ab Seite 96 beschrieben.

5.1.6. User Authentication

Benutzerauthentifizierung (User Authentication) ist auf diesem Internet-Sicherheitssystem mit den Proxydiensten HTTP, SMTP und SOCKSv5 möglich. Es kann festgelegt werden, welcher Benutzer diese Proxydienste in Anspruch nehmen darf. Die Benutzer-Accounts können lokal auf dem System im Menü **Definitions/Users** angelegt werden. Es können aber auch externe Benutzer-Datenbanken abgefragt werden. Unterstützt werden die Authentifizierungsmethoden **RADIUS**, **SAM** (Windows NT/Windows 2000/XP-Server), **Microsoft Active Directory** und **OpenLDAP**. Dies kann von Vorteil sein, wenn bereits eine Benutzerdatenbank auf einem solchen Server vorhanden ist, und die Benutzer somit nicht noch einmal auf dem Internet-Sicherheitssystem eingetragen werden müssen.

Die Authentifizierung des Clients bei Anfragen an einen Proxydienst muss durch Benutzernamen und Passwort erfolgen. Auf diese Weise wird die Authentifizierung personenbezogen (User) und nicht IP-bezogen durchgeführt. Dies ermöglicht ein personenbezogenes **Accounting** im HTTP-Proxy Zugangsprotokoll.

Proxydienste und Authentifizierungsmethoden

Die Proxydienste **HTTP**, **SMTP** und **SOCKSv5** können so konfiguriert werden, dass sie alle Clients (auf IP-Adressen basierend) oder nur Clients mit einem gültigen Benutzernamen und Passwort (Benutzerauthentifizierung) akzeptieren. Wenn Sie **User Authentication** aktivieren, müssen Sie mindestens eine Methode für Ihr System auswählen, um die angefragten Berechtigungsnachweise zu bewerten. Ansonsten können Sie den Proxydienst nicht benutzen.

Das System unterstützt Benutzerauthentifizierung mit ...

- einem RADIUS-Server
- einer NT SAM Benutzer-Basis
- einem LDAP-Server
- einer lokalen Benutzerdatenbank im WebAdmin

Die vier Benutzerdatenbanken können nacheinander abgefragt werden.

5.1.6.1. RADIUS

RADIUS steht für **Remote Authentication Dial In User Service** und ist ein Protokoll, mit dem z. B. ein ISDN-Router Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen kann. Neben den reinen Benutzerinformationen für die Authentifizierung verwaltet RADIUS auch technische Informationen, die für die Verständigung des Zugangssystems mit dem Endgerät des Anrufers nötig sind. Dazu gehören z. B. die verwendeten Protokolle, IP-Adressen, Telefonnummern, Time-outs, Routen etc. Zusammen bilden sie ein Benutzerprofil, das in einer Datei oder Datenbank auf dem RADIUS-Server gespeichert wird.
Neben der Authentifizierung von DialUp-Usern kann **RADIUS** aber auch als generisches Authentifizierungsprotokoll verwendet werden.

Das Protokoll ist sehr flexibel und die RADIUS-Server sind für alle Betriebssysteme eingeschlossen Microsoft Windows NT/2000 verfügbar. Die RADIUS-Implementierung dieses Internet-Sicherheitssystems ermöglicht Ihnen die Zugriffsrechte auf Proxy- und Benutzerbasis zu konfigurieren.

Bevor Sie **RADIUS**-Authentication einstellen können, benötigen Sie einen RADIUS-Server in Ihrem Netzwerk. Da die Passwörter in Klartext übertragen werden, empfehlen wir jedoch, den RADIUS-Server ausschließlich in einer geswitchten Umgebung zu verwenden.

Im folgenden Abschnitt wird als Beispiel detailliert das Einrichten von Microsofts IAS (RADIUS-Server für MS Windows NT und 2000) beschrieben. Falls Sie einen anderen RADIUS-Server verwenden, benötigen Sie die folgenden Informationen, um den Betrieb mit der Benutzerauthentifizierung des Internet-Sicherheitssystems zu ermöglichen.

Die Authentifizierungsanfrage enthält drei gesetzte Felder:

- Benutzername
- Passwort in Klartext (PAP)
- Proxyart (String **http**, **smtp** oder **socks**) im Feld **NAS-Identifier**

Der RADIUS-Server muss anhand dieser Informationen entscheiden, ob der Zugriff auf den Proxy bewilligt wird, und eine entsprechende Antwort zurückliefern.

Microsofts IAS RADIUS-Server einstellen:

IAS wird mit allen Microsoft Windows 2000 Server-Versionen ausgeliefert, ist aber standardmäßig meist nicht installiert. Für Microsoft Windows NT4 ist **IAS** Bestandteil von **NT4 Option Pack** und ist ohne Aufpreis erhältlich. Die MS Windows NT4 IAS-Version hat weniger Features als die 2000er-Version, jedoch reicht diese für die gebräuchlichen Authentifizierungs-Einstellungen dieses Internet-Sicherheitssystems vollkommen aus.

1. Installieren Sie den **IAS**-Dienst, falls er nicht bereits installiert ist.

2. Legen Sie für jeden Proxy, der verwendet werden soll, eine Benutzergruppe an.

   Tipp:

   Benennen Sie die Gruppe entsprechend des zugeordneten Proxydienstes. Die Gruppe für den HTTP-Proxy könnte z. B. **HTTP-Proxybenutzer** lauten.

3. Nun ordnen Sie dieser Gruppe alle Benutzer zu, die in der Lage sein sollen, den entsprechenden Proxy zu benutzen.

4. Stellen Sie sicher, dass bei allen Benutzern in diesen Gruppen das Benutzerflag **Einwahlzugriff auf das Netzwerk erlauben** aktiviert ist.
   Diese Einstellung finden Sie in den Benutzereigenschaften. MS Windows NT/2000 benötigt dieses Flag, um RADIUS-Anfragen positiv zu beantworten.

5. Öffnen Sie das Verwaltungsprogramm für den **IAS**-Dienst.

6. Fügen Sie einen Client hinzu. Dazu müssen Sie folgende Angaben machen:

   Beliebiger Client-Namen: Tragen Sie hier den **DNS**-Namen Ihres Internet-Sicherheitssystems ein.

   Protokoll: Wählen Sie hier **RADIUS** aus.

   IP-Adresse des Clients: Dies ist die interne IP-Adresse Ihres Internet-Sicherheitssystems.

Client Vendor: Tragen Sie hier **RADIUS Standard** ein.

Shared Secret: Tragen Sie ein beliebiges Passwort ein. Dieses Passwort benötigen Sie später zur Konfiguration des RADIUS-Servers im Konfigurationstool **WebAdmin**.

Sicherheitshinweis:

Für das **Shared Secret** werden nur Passwörter bestehend aus alphanumerischen sowie Minus- und Punkt-Zeichen unterstützt.
Sonderzeichen, z. B. %!#_{} sind nicht möglich.

7. Wechseln Sie nun zum Menü **RAS-Richtlinien**.
Hier ist eine Standardrichtlinie eingetragen. Wenn Sie **IAS** nur für das Internet-Sicherheitssystem verwenden wollen, können Sie diese löschen.

   Tragen Sie nun für jeden Proxy eine Richtlinie ein. Auf diese Weise können Sie den Namen entsprechend wählen, z. B. HTTP-Zugriff.

   Fügen Sie zwei Bedingungen hinzu:

   1. Bedingung: Das Feld NAS-Identifier muss einem String laut folgender Tabelle entsprechen.

Proxytyp	NAS-Identifier entspricht String
HTTP	http
SOCKS	socks
SMTP	smtp
WebAdmin Access	webadmin
Surf Protection	"Profilname"
PPTP	"kein Identifier eintragen"

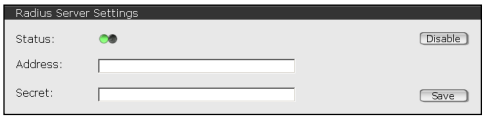
   2. Bedingung: Die Windows-Gruppe des zugreifenden Benutzers muss der in Schritt 2 angelegten Benutzergruppe entsprechen.

   Nur wenn vom Benutzer beide Bedingungen erfüllt werden, wird der Zugriff erlaubt.

8. Bearbeiten Sie das Profil der Richtlinie, indem Sie unverschlüsselte Authentifizierung erlauben (PAP).
Belassen Sie bei allen anderen Profil-Einstellungen die voreingestellten Werte.

9. Starten Sie das Konfigurationstool **WebAdmin** und öffnen im Verzeichnis **System** das Menü **User Authentication**.

10. Schalten Sie die Funktion im Fenster **RADIUS Server Settings** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein (Statusampel zeigt Grün).



Address: Tragen Sie hier die IP-Adresse des RADIUS-Servers ein.

Secret: Tragen Sie hier das Passwort **Shared Secret** aus Schritt 6 ein.

11. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

12. Öffnen Sie das Menü des entsprechenden Proxys, bei dem Benutzerauthentifizierung mittels RADIUS erfolgen soll.

13. Falls **User Authentication** noch ausgeschaltet ist (Statusampel zeigt Rot), aktivieren Sie diese, indem Sie auf die Schaltfläche **Enable** klicken.

    Authentication methodes: Wählen Sie in diesem Auswahlfeld RADIUS aus.

14. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Die Benutzerauthentifizierung per **RADIUS** ist nun aktiviert.
Im Microsoft Windows NT/2000 **Event Log** protokolliert anschließend der IAS-Server jeden Zugriff auf den Proxyserver.

Um ein schnelles Volllaufen des Event-Logs zu verhindern, speichert das Internet-Sicherheitssystem die vom RADIUS-Server gelieferten Daten für fünf Minuten. Das bedeutet allerdings auch, dass sich Änderungen an der Benutzerdatenbank gegebenenfalls erst nach maximal fünf Minuten bemerkbar machen.

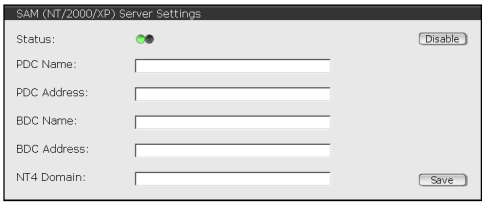
Achtung:

Das Internet-Sicherheitssystem sendet Anfragen über den UDP-Port 1812.

5.1.6.2. SAM – NT/2000/XP

Bei dieser Authentifizierungsmethode wird zur Bewertung der Anfragen ein MS Windows NT/2000 Domain Controller oder ein Stand-alone-Server verwendet. Viele Unternehmen verwenden bereits MS Windows NT/2000-Netzwerke, die auf dem MS Windows NT/2000 Active Directory-Domain-Konzept basieren.
Der Vorteil von SAM ist, dass es sehr einfach zu konfigurieren ist, wenn auf dem Netzwerk schon ein **Primary Domain Controller (PDC)** oder ein einfacher Server mit Benutzerdatenbank läuft.
Der Nachteil ist, dass bei diesem Modell nicht zwischen verschiedenen Benutzergruppen unterschieden werden kann. Sie können entweder alle Benutzer einer SAM-Datenbank für einen bestimmten Proxy freischalten oder keinen.

SAM – NT/2000/XP einstellen:



Um diese Authentifizierungsmethode zu verwenden, benötigen Sie einen Microsoft Windows NT- oder 2000-Server in Ihrem Netzwerk, der die Benutzer-Daten enthält. Dies kann entweder ein Primary Domain Controller (PDC) oder ein selbständiger Server sein.

Dieser Server hat einen NETBIOS-Namen (der NT/2000 Servername) und eine IP-Adresse.

1. Öffnen Sie im Verzeichnis **System** das Menü **User Authentication**.

2. Schalten Sie die Funktion im Fenster **SAM (NT/2000/XP) Server Settings** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   PDC Name: Tragen Sie in dieses Eingabefeld den Namen des Domain-Controllers ein.
   Da ab Microsoft Windows 2000 diese Namen auch offizielle **DNS**-Namen sind, unterstützen wir nur Namen bestehend aus alphanumerischen sowie Minus- und Punkt-Zeichen.
   Sonderzeichen, z. B. %!#_{} werden als Fehler gewertet.

PDC Address: Tragen Sie in dieses Eingabefeld die IP-Adresse des Domain-Controllers ein.

BDC Name: Wenn Sie einen Backup Domain Controller verwenden, tragen Sie in dieses Eingabefeld den Namen ein. Falls Sie keinen BDC verwenden, tragen Sie hier den Namen des PDC ein.

BDC Address: Tragen Sie in dieses Eingabefeld die IP-Adresse des Backup Domain Controllers ein. Falls Sie keinen BDC verwenden, tragen Sie hier die IP-Adresse des PDC ein.

NT4 Domain: Tragen Sie hier den Namen Ihrer MS Windows NT/ 2000-Domain ein.
Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, das Minus-Zeichen und Unterstrich.

Hinweis:

Dies ist keine Internet-Domain, wie etwa Firma.de, sondern ein einfacher Bezeichner, z. B. **Intranet**. Falls Sie das Microsoft Domain-Konzept nicht benutzen, sondern nur einen einfachen Server haben, tragen Sie hier den NETBios-Namen des Servers ein. Dies entspricht dem Eintrag im Eingabefeld **PDC Name**.

3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Sicherheitshinweis:

Wenn Sie SAM-Authentifizierung verwenden, sollten Sie den **Guest**-Account Ihrer Windows-Domain deaktivieren, da sonst alle Benutzer/Passwort-Kombinationen als gültig angesehen werden!

5.1.6.3. LDAP Server

LDAP steht für **Lightweight Directory Access Protocol** und ist ein Kommunikationsprotokoll das den Transport und das Format von Nachrichten definiert, die von einem Client für den Zugriff auf einen X.500-konformen Verzeichnisdienst verwendet werden. Das Protokoll spezifiziert somit die Art des Zugriffs auf einen solchen Verzeichnisdienst.

Bei diesem Internet-Sicherheitssystem wird das Protokoll **LDAP** zur Benutzerauthentifizierung eingesetzt, indem mit Hilfe von Stand-alone-LDAP-Servern Verzeichnisse nach einem Benutzer mit einer bestimmten Gruppenzugehörigkeit oder mit bestimmten Attributen abgefragt werden.
Das System unterstützt die Stand-alone-LDAP-Server **Microsoft Active Directory** und **Novell eDirectory** sowie LDAP-Server, die auf der Open-Source-Implementation von **OpenLDAP** basieren.

Microsoft Active Directory ist der Verzeichnisdienst speziell für Microsoft Windows NT/2000-Netzwerke und erlaubt die zentrale Organisation und Verwaltung aller Netzwerkressourcen. Er ermöglicht den Benutzern über eine einzige zentrale Anmeldung den Zugriff auf alle Ressourcen und dem Administrator die zentral organisierte Verwaltung, transparent von der Netzwerktopologie und den eingesetzten Netzwerkprotokollen.
Für diesen Verzeichnisdienst wird zur Bewertung der Anfragen ein MS Windows NT/2000 Domain Controller benötigt.

Novell eDirectory – Novell Directory Service 8 - ist ein auf X.500 basierender Verzeichnisdienst zur Verwaltung von Benutzern, Zugriffsrechten und anderen Netzwerkressourcen. Novell stellt den Verzeichnisdienst für die Plattformen Netware ab Version 5, MS Windows NT/2000, Linux und Solaris zur Verfügung.

Mit Hilfe des Open-Source-Projekts **OpenLDAP**, das unter der Aufsicht der **OpenLDAP Foundation** realisiert wird, kann in einem Netzwerk ein Verzeichnisdienst mit unterschiedlichen Stand-alone-LDAP-Servern aufgebaut werden. Auf der Open-Source-Software basiert z. B. der Stand-alone-LDAP-Server **iPlanet Directory Server**.

Benutzerauthentifizierung

Bei der Benutzerauthentifizierung über **LDAP** wird im Verzeichnisdienst der **Distinguished Name (DN)** des Benutzers abgefragt. Der abgefragte Name des Benutzers muss innerhalb des Verzeichnisses einmalig sein.

Bei **Microsoft Active Directory (AD)** und **Novell eDirectory (NDS8)** hat jedes Objekt einen definierten **DN**, der die Domain und den Pfad im AD-Verzeichnis, bzw. im NDS-Baum identifiziert und in der Gesamtstruktur eindeutig ist. Dieser **DN** setzt sich aus **Common Name (CN)** und **Domain Component (DC)** zusammen.
Beispiel: CN=Administrator, CN=Users, DC=example, DC=com

Unter **MS Active Directory** kann die Benutzerauthentifizierung auch durch den **User Principal Name (UPN)** erfolgen. Dieser Name besteht aus dem Anmeldenamen und dem DNS-Namen der Domain.
Beispiel: admin@example.com

Unter **OpenLDAP** erfolgt eine einfache Abfrage nach dem **Common Name (CN)**. Hierbei ist zu beachten, dass jedem eingetragenen Benutzer ein eindeutiger **CN** zugeordnet sein muss.

Sicherheitshinweis:

Bei der Benutzerauthentifizierung mittels Stand-alone-LDAP-Server werden ausschließlich Klartextpasswörter verwendet und während der Anfrage nicht mit SSL verschlüsselt. Somit ist es in ungeswitchten Umgebungen möglich, Passwörter, die vom Internet-Sicherheitssystem gesendet werden mitzulesen.

Hinweis:

Für die Benutzerauthentifizerung mittels **LDAP-Server** muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

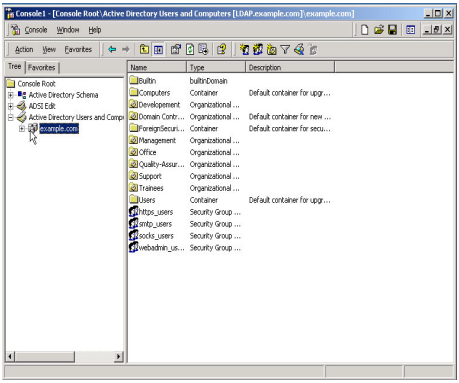
Microsoft Active Directory-Server einstellen:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

Bei **Microsoft Active Directory (AD)** sollte der Abfrage-Typ **MemberOf** verwendet werden, da sich ein bereits vollständig eingerichteter Verzeichnisdienst einfach erweitern lässt.
Das Verzeichnis (Directory) kann wiederum um selbstdefinierte Attribute erweitert werden. Diese Attribute, die für jeden Benutzer einzeln auf dem Directory-Server gesetzt werden müssen, geben durch den Wert oder den Inhalt Auskunft welche Berechtigungen dem Benutzer zugewiesen wurden.



In diesem Konfigurations-Beispiel wird die kleine Domain **example.com** dargestellt:

Im Verzeichnis **Trainees** befindet sich der Benutzer **Hans Mustermann**.
DN: cn=hans mustermann, ou=trainees, dc=example, dc=com.
LogonName: mustermann@example.com

Dieser Benutzer könnte sich mit seinem LogonName und seinem Passwort z. B. am SOCKS-Proxy anmelden. Das Internet-Sicherheitssystem überprüft in diesem Fall den DN und das Passwort von Hans Mustermann. Falls es dann zum LogonName mustermann@example.com einen eindeutigen DN gibt, und das eingegebene Passwort gültig ist, kann der Benutzer den Dienst SOCKS verwenden.

Falls Sie den Abfrage-Typ **MemberOf** verwenden möchten, führen Sie am Stand-alone-LDAP-Server **Microsoft Active Directory** folgende Einstellungen durch:

Schritt 1 - Erstellen einer Security Group:

1. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf die Domain.

   Beispiel: Domain **example.com**

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **New** und anschließend auf **Group**.

   Anschließend öffnet sich das Fenster **New Object - Group**.

3. Definieren Sie im Eingabefeld **Group name** einen eindeutigen Namen für die Gruppe.

   Beispiel: **socks_users** für den SOCKS-Proxy

4. Wählen Sie bei **Group type** die Option **Security** aus.

5. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

   Sie haben nun die neue **Security Group** mit dem Namen **socks_users** erstellt.

Schritt 2 - Benutzer der Security Group zuweisen:

1. Wählen Sie im Verzeichnis den Benutzer aus und klicken mit der rechten Maustaste auf den Namen.

   Beispiel: **Hans Mustermann** im Verzeichnis **Trainees**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Properties**.

   Anschließend öffnet sich das Fenster **Properties**.

3. Wählen Sie im Fenster **Properties** das Register **MemberOf** aus.

4. Um die neue Gruppe auszuwählen, klicken Sie auf die Schaltfläche **Add**.

5. Anschließend öffnet sich das Fenster **Select Groups**.

6. Wählen Sie nun die **Security Group** aus.

Beispiel: **socks_users**

7. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **OK**.

   Die neue **Security Group** wurde nun in das Fenster **MemberOf** übernommen.

8. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Führen Sie nun die Einstellungen am Internet-Sicherheitssystem durch. Die Einstellungen am Konfigurationstool **WebAdmin** werden ab Seite 82 erklärt.

Microsoft Active Directory, selbstdefinierte Attribute:

Die Benutzerauthentifizierung mittels Microsoft Active Directory kann auch mit zusätzlich selbstdefinierten Attributen und Werten erfolgen. Die Konfiguration ist allerdings sehr viel aufwendiger.

Hinweis:

Um eine derartige Erweiterung unter MS Active Directory durchzuführen, benötigen Sie für jedes Attribut eine **Objekt ID (OID)**. Die OID-Nummer ist im gesamten Internet einzigartig und wird an Unternehmen von der **Internet Assigned Numbers Authority (IANA)** ausgestellt. Die OID der Astaro AG ist z. B. `1.3.6.1.4.1.9789`.

Falls Sie noch keine OID-Nummer haben, können Sie diese direkt bei der **IANA** unter der Internetadresse **www.iana.org** beantragen.
Überlegen Sie im ersten Schritt, wie Sie diese OID-Nummer am besten Ihrer Netzwerkstruktur anpassen und erweitern. Beachten Sie, dass für jedes Benutzerattribut eine eigene OID benötigt wird.

Für die Erstellung weiterer Attribute muss die **Microsoft Management Console** zuvor um das **Active Directory Schema** ergänzt werden. Des Weiteren müssen Sie gewährleisten, dass Sie dieses Schema bearbeiten bzw. erweitern und verändern dürfen.

Schritt 1 – Active Directory Schema freigeben:

1. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf **Active Directory Schema**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Operations Master**.

   Anschließend öffnet sich das Fenster **Change Schema Master**.

3. Markieren Sie das Optionsfeld **The Schema may be modified on this Domain Controller**.

4. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **OK**.

   Sie sind nun berechtigt, das **Active Directory Schema** zu bearbeiten.

Schritt 2 – Neues Attribute erstellen:

1. Klicken Sie mit der rechten Maustaste unter **Active Directory Schema** auf das Verzeichnis **Attribute**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **New**.

3. Definieren Sie im Fenster **Create New Attribute** das neue Attribut.

   Common Name: Tragen Sie in das Eingabefeld den **CN** ein.

   LDAP Display Name: Vergeben Sie für das neue Attribut einen eindeutigen Namen. Am Besten denselben Namen, den Sie für diesen Dienst (Service) auch auf dem Internet-Sicherheitssystem verwendet haben.
   Beispiel: **Socks**.

   Unique X500 Object ID: Tragen Sie in das Eingabefeld die OID-Nummer ein.

   Syntax: Wählen Sie **Boolean** aus.

   Minimum: Lassen Sie dieses Eingabefeld leer.

   Maximum: Lassen Sie dieses Eingabefeld leer.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Schritt 3 – Attribut einer Klasse (Class) zuweisen:

1. Klicken Sie mit der linken Maustaste unter **Active Directory Schema** auf das Verzeichnis **Classes**.

2. Klicken Sie mit der rechten Maustaste auf das Verzeichnis **Users**.

   Anschließend öffnet sich das Fenster **User Properties**.

3. Klicken Sie auf das Register **Attributes** und führen Sie die folgenden Einstellungen durch.

   Optional: Wählen Sie im Auswahlfeld das Attribut aus und übernehmen Sie dieses durch einen Klick auf die Schaltfläche **Add**.
   Beispiel: **Socks**.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

5. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf **Active Directory Schema**.

6. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Reload the Schema**.

Schritt 4 – Attribut einem Benutzer (User) zuweisen:

1. Klicken Sie im Verzeichnis **ADSI Edit** mit der rechten Maustaste auf den entsprechenden Benutzer.

   Beispiel: **Hans Mustermann** im Verzeichnis **Trainees**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Properties**.

   Anschließend öffnet sich das Fenster **Properties**.

3. Wählen Sie im Fenster **Properties** das Register **Attributes** aus und führen Sie die folgenden Einstellungen durch.

   Select which properties to view: Wählen Sie **Both** aus.

   Select a property to view: Wählen Sie hier das Attribut aus. Beispiel: **Socks**.

Syntax: Dieser Wert wird beim Erstellen des Attributs gesetzt und kann hier nicht mehr geändert werden.
Beispiel lt. Schritt 2: **Boolean**.

Edit Attribut: Mit diesem Eingabefeld kann der Wert des Attributs editiert werden. Mögliche Werte sind **TRUE** oder **FALSE**.

Value(s): Hier wird der Wert des Attributs angezeigt.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Führen Sie nun die Einstellungen am Internet-Sicherheitssystem durch. Die Einstellungen im Konfigurationstool **WebAdmin** werden ab Seite 82 erklärt.

Novell eDirectory-Server einstellen:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Sicherheitshinweis:
Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

Bei **Novell eDirectory (NDS8)** sollte der Abfrage-Typ **group-Membership** verwendet werden, da sich ein bereits vollständig eingerichteter Verzeichnisdienst einfach erweitern lässt.
Das Verzeichnis kann wiederum um selbstdefinierte Attribute erweitert werden. Diese Attribute, die für jeden Benutzer einzeln auf dem Directory-Server gesetzt werden müssen, geben durch den Wert oder den Inhalt Auskunft welche Berechtigungen dem Benutzer zugewiesen wurden.
Für die Konfiguration des Novell eDirectory-Servers benötigen Sie die **Novell ConsoleOne**.

Die Verwaltung des Novell eDirectory-Servers wird ausführlich in der zugehörigen Dokumentation beschrieben. Sie erhalten die Dokumentation unter der Internetadresse:

http://www.novell.com/documentation/lg/edir87/index.html

Führen Sie anschließend die Einstellungen am Internet-Sicherheitssystem durch. Die Einstellungen am Konfigurationstool **WebAdmin** werden ab Seite 82 erklärt.

OpenLDAP-Server konfigurieren:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

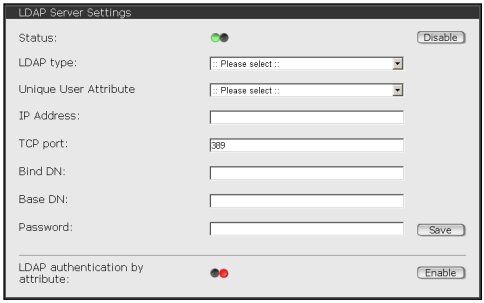
Unter **OpenLDAP** erfolgt zur Benutzerauthentifizierung eine einfache Abfrage nach dem **Common Name (CN)**. Hierbei ist zu beachten, dass jedem eingetragenen Benutzer ein eindeutiger **CN** zugeordnet sein muss.

Wichtiger Hinweis:

Stellen Sie sicher, dass jeder Benutzer in dem **OpenLDAP**-Verzeichnis einen eindeutigen **Common Name (CN)** erhält.

Da es verschiedene Stand-alone-LDAP-Server gibt, die auf dem Open-Source-Projekt **OpenLDAP** basieren, entnehmen Sie die Informationen zur Installation und Konfiguration dieser Verzeichnisse der entsprechenden Dokumentation.
Falls Sie den Stand-alone-LDAP-Server **SLAPD** der **OpenLDAP Foundation** verwenden, erhalten Sie die aktuelle Dokumentation unter der Internetadresse: **http//www.openldap.org**.

LDAP auf Internet-Sicherheitssystem einstellen:



Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Um die nötigen Einstellungen auf dem Internet-Sicherheitssystem durchzuführen, benötigen Sie den **Distinguished Name (DN)** dieses Benutzers

sowie den LDAP-Type und die IP-Adresse des Stand-alone-LDAP-Servers.

Sicherheitshinweis:

Stellen Sie sicher, dass der Benutzer **nur** die Leserechte für den Stand-alone-LDAP-Server bekommt.

1. Öffnen Sie im Verzeichnis **System** das Menü **User Authentication**.

2. Schalten Sie die Funktion im Fenster **LDAP Server Settings** durch einen Klick auf die Schaltfläche **Enable** bei **Status** ein.

   LDAP Type: Wählen Sie in diesem Drop-down-Menü den Type des Stand-alone-LDAP-Servers aus.
   Die möglichen Typen sind: **Microsoft Active Directory**, **Novell eDirectory** und **OpenLDAP**.

   Unique User Attribute: Dieses Atribut definiert den Benutzernamen zur Authentifizierung am Stand-alone-LDAP-Server. Die zur Verfügung stehenden Atribute hängen vom ausgewählten Type des Stand-alone-LDAP-Servers ab. Falls Sie für den Benutzernamen ein eigenes Attribut erstellen möchten, wählen Sie hier **Selfdefined** aus (siehe nachfolgendes Bild).

   Für den LDAP-Server **Microsoft Active Directory** können Sie das Atribut **User Principal Name (UPN)** oder **saMAccountName** auswählen.

   Für die LDAP-Server **Novell eDirectory** und **OpenLDAP** kann jeweils das Attribut **Common Name (CN)**, **Surname (SN)** oder **Unique Identifier (UID)**.

Attribute Name: Dieses Eingabefeld wird nur angezeigt, wenn im Drop-down-Menü **Unique User Attribute** die Einstellung **Selfdefined** ausgewählt wurde.

Definieren Sie in diesem Eingabefeld das eigene Attribut zur Bestimmung des Benutzernamens.

IP Address: Tragen Sie in das Eingabefeld die IP-Adresse des Stand-alone-LDAP-Servers ein.

TCP port: Tragen Sie in das Eingabefeld den TCP Port ein. Per Default ist der Standard-Port 389 bereits eingetragen.

Bind DN: Der hier einzutragende Wert hängt vom Type des Stand-alone-LDAP-Servers ab:

1. Microsoft Active Directory

Sie können den **User Principal Name (UPN)** oder den gesamte **Distinguished Name (DN)** des Benutzers eintragen.
Beispiele:
UPN: admin@example.com
DN: cn=administrator, cn=users, dc=example, dc=com

2. Novell eDirectory

Tragen Sie in das Eingabefeld den gesamten **Distinguished Name (DN)** des Benutzers ein.
Beispiel:
DN: cn=administrator, o=our_organisation

3. OpenLDAP

Bei **OpenLDAP** oder OpenLDAP-konformen Stand-alone-Servern, kann nur der **Distinguished Name (DN)** des Benutzers eingetragen werden.

Base DN: Tragen Sie in das Eingabefeld die Objektnamen ein, von wo aus der Client den Vorgang startet.
Beispiele:
Für MS Active Directory: dc=example, dc=com
Für Novel eDirectory: o=our_organisation

3. Tragen Sie im Eingabefeld **Password** das Passwort ein. Dieses Passwort sollte auch für die Administration des Stand-alone-LDAP-Servers verwendet werden.

Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35$4.

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Sicherheitshinweis:

Solange die Funktion **LDAP authentication by attribute** ausgeschaltet ist, können alle Benutzer, die im Verzeichnisdienst einen eindeutigen **DN** und ein gültiges Passwort haben die Proxies **HTTP**, **SMTP** und **SOCKS** verwenden sowie auf das Konfigurationstool **WebAdmin** zugreifen.

LDAP, erweiterte Authentifizierung:

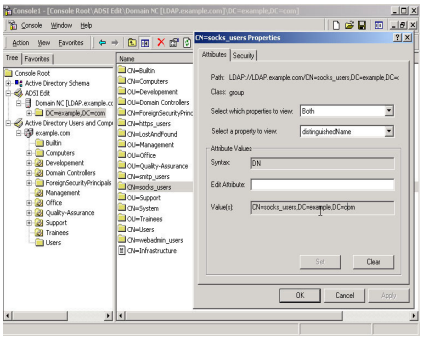
1. Schalten Sie die Funktion **LDAP authentication by attribute** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

2. Wählen Sie im Drop-down-Menü **Service** den Dienst aus.

   Die möglichen Dienste sind: **HTTP**, **SMTP**, **SOCKS** und **WebAdmin**.

3. Tragen Sie in das Eingabefeld **Attribute Name** den Attributnamen ein.
   Falls Sie einen **Microsoft Active Directory**-Server verwenden und den Abfrage-Typ **MemberOf** konfiguriert haben, ist dies der Name der entsprechenden **Security Group**.
   Beispiel: **socks_users**.

4. Tragen Sie in das Eingabefeld **Attribute Value** den Attributwert ein. Der Attributwert ist der **DN**.



Bei **Microsoft Active Directory** wird der **DN** des Attributs über die **Management Console** im Verzeichnis **ADSI Edit** angezeigt: Wählen Sie über den **Base DN** (Beispiel: dc=example, dc=com) den Attributnamen (Beispiel: socks _users) aus und klicken darauf mit der rechten Maustaste. Das Fenster **CN=socks_users Properties** wird geöffnet.

Wählen Sie nun im Drop-down-Menü **Select which properties to view** den Wert **Both** und im Drop-down-Menü **Select a property to view** den Wert **distinguishedName** aus. Der im Feld **Value(s)** angezeigte Wert ist der Attributwert.

5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Nun ist jeder Benutzer, der als **MemberOf** der Security Group **socks_users** definiert wurde berechtigt diesen Dienst zu verwenden.

5.1.7. WebAdmin Site Certificate

Ein wichtiger Bestandteil des Internet-Sicherheitssystems sind die Verschlüsselungsverfahren. Diese kryptographischen Verfahren werden bei der Übertragung vertraulicher Daten über **Virtual Private Networks** (Kapitel 5.6 ab Seite 209), der **Benutzerauthentifizierung** und beim **Up2Date Service** sowie zur sicheren Administration des Internet-Sicherheitssystems angewendet.

Zertifikate und Certificate Authorities (CA) sind ein wesentlicher Bestandteil moderner kryptografischer Anwendungen und schließen die Sicherheitslücken, die bei anderen Algorithmen alleine noch offen bleiben. Eine sehr elegante Art verschlüsselt zu kommunizieren, sind die **Public-Key**-Algorithmen. Sie setzen jedoch voraus, dass die öffentlichen Schlüssel aller Partner bekannt sind.
Hier kommt eine vertrauenswürdige dritte Stelle ins Spiel, die für die Echtheit öffentlicher Schlüssel sorgt. Zu diesem Zweck stellt sie Zertifikate aus. Diese Stelle wird daher auch **Cerficate Authority (CA)** genannt. Ein Zertifikat ist ein Datensatz oder ein Text in einem standardisierten Format mit den wichtigsten Daten des Besitzers, seinem Namen und seinem öffentlichen Schlüssel, unterschrieben mit dem privaten Schlüssel der **CA**. Das Format der Zertifikate ist im X.509-Standard festgelegt.
In einem Zertifikat unterschreibt die **CA**, dass sie sich von der Echtheit einer Person überzeugt hat und dass der vorliegende öffentliche Schlüssel zu der Person gehört. Da das Zertifikat Werte wie den Namen des Besitzers, die Gültigkeitsdauer, die ausstellende Behörde und einen Stempel mit einer Unterschrift der Behörde enthält, kann es auch als digitaler Pass betrachtet werden.

Mit Hilfe dieses Menüs erzeugen Sie zwei Zertifikate: Zum einen das CA-Zertifikat, welches im Zertifikatspeicher Ihres Browsers installiert wird und zum anderen ein Server-Zertifikat, das wiederum das Internet-Sicherheitssystem benötigt, um sich bei Ihrem Browser zu authentifizieren. Diese zwei Zertifikate prüfen die Firmendaten und den Sicherheitssystem-Hostnamen.

Zertifikat für WebAdmin erstellen:

1. Öffnen Sie im Verzeichnis **System** das Menü **WebAdmin Site Certificate**.

2. Tragen Sie im Fenster **Certificate Information** die entsprechenden Firmendaten in das Drop-down-Menü und die Eingabefelder ein.

   Country Code: Wählen Sie in diesem Drop-down-Menü das Land aus.

   State or Region: Tragen Sie das Bundesland ein.

   Company: Tragen Sie den Firmennamen ein.

   Org. Unit: Tragen Sie die Abteilung Ihrer Firma ein.

   Contact E-Mail: Tragen Sie die E-Mail-Adresse ein, über die Sie eventuell kontaktiert werden möchten.

3. Tragen Sie in das Eingabefeld **Firewall Hostname** den Hostnamen oder die IP-Adresse des Sicherheitssystems ein, über die Sie mit Ihrem Browser auf **WebAdmin** zugreifen.

   Beispiel: Wenn Sie über die Adresse https://192.168.10.1 auf das Konfigurationstool **WebAdmin** zugreifen, tragen Sie 192.168.10.1 in das Eingabefeld ein.

4. Speichern Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Zertifikat für WebAdmin installieren:

1. Um nun das CA-Zertifikat auf Ihrem Browser zu installieren, klicken Sie Fenster **CA Certificate Installation** auf die Schaltfläche **Import Certificate into Browser**.

   Die anschließenden Dialoge sind von Ihrem Browsertyp abhängig. Bei Microsoft Internet Explorer z. B. öffnet sich der Dialog **Dateidownload**:

   Datei auf Datenträger speichern: Mit dieser Option können Sie das Zertifikat vor der Installation auf einem lokalen Datenspeicher sichern.

   Die Datei von ihrem aktuellen Ort öffnen: Mit dieser Option wird das Zertifikat direkt geöffnet. Im Fenster **Zertifikat** haben Sie anschließend drei Register zur

Verfügung. In diesen Registern können Sie die Daten Ihres Zertifikats betrachten und anschließend installieren.

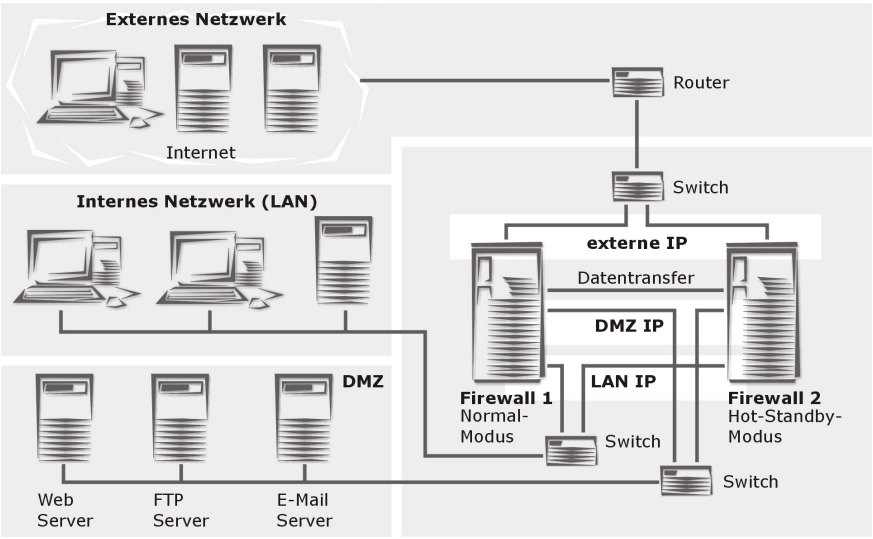
2. Um den jeweiligen Vorgang zu starten, klicken Sie auf die Schaltfläche **OK**.

Hinweis:

Infolge von unterschiedlichen Systemzeiten und den weltweit versetzten Zeitzonen, kann es vorkommen, dass das Zertifikat nicht sofort gültig ist. Viele Browser versenden dann die Meldung, dass das Zertifikat abgelaufen sei. Diese Meldung ist nicht richtig. Das neu generierte Zertifikat wird nach maximal 12 Stunden gültig.

5.1.8. High Availability

Der häufigste Grund für den Ausfall eines Internet-Sicherheitssystems, bzw. einer Firewall ist ein Defekt der Hardware, z. B. des Netzteils, der Festplatte oder des Prozessors. Bei diesem **High Availability (HA)**-System werden zwei Internet-Sicherheitssysteme mit identischer Hardware parallel geschaltet. Das Firewall-System 1 läuft im Normal-Modus (Master). Das Firewall-System 2 befindet sich im Hot-Standby-Modus (Slave) und überwacht das aktive Sicherheitssystem über die Datentransfer-Leitung mittels Link Beat. Das Firewall-System 1 schickt über diese Verbindung in regelmäßigen Abständen Heart-Beat-Anfragen, die vom Firewall-System 2 beantwortet werden. Über die Datentransfer-Leitung wird das Firewall-System 2 bei Bedarf auch aktualisiert, damit es bei einem Ausfall des aktiven Systems sofort deren Funktion übernehmen kann.



Hardware- und Software-Voraussetzungen

- Die High Availability (HA)-Lizenz
- 2 Internet-Sicherheitssysteme mit identischer Hardware
- 2 zusätzliche Ethernet Netzwerkkarten für die Datentransfer-Leitung (falls die Überwachung mittels Heart-Beat-Anfragen erfolgen soll, benötigen Sie hier 2 link-beat-fähige Ethernet Netzwerkkarten)
- Ein Ethernet Crossover-Kabel
- Ein Serielles Schnittstellenkabel (optional)

Wichtiger Hinweis:

Für die Überwachung mittels Heart-Beat-Anfragen über die Datentransfer-Leitung werden link-beat-fähige Netzwerkkarten benötigt. Die vom Internet-Sicherheitssystem unterstützten Hardware-Komponenten sind unter der Internetadresse **http://docs.astaro.org** im Verzeichnis **Hardware Compatibility List for Astaro Security Linux** aufgelistet.

High Availability-System installieren

Vorbereitung:

1. Installieren Sie zuerst die Software auf den beiden Rechnern und konfigurieren das Firewall-System 1 wie in Kapitel 3.2 ab Seite 21 beschrieben.

   Wichtiger Hinweis:

   Falls Sie das **High Availability (HA)**-System nachträglich installieren, achten Sie darauf, dass das System 2 auf die selbe Version wie System 1 upgedated wird.

2. Fahren Sie beide Systeme herunter.

3. Schließen Sie das Firewall-System 2 an das Firewall-System 1, wie in der Grafik dargestellt, an.

Firewall-System 1 (Normal-Modus) konfigurieren:

4. Starten Sie das System 1.

5. Öffnen Sie im Verzeichnis **System** das Menü **High Availability**.

6. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Name of the device: Tragen Sie in das Eingabefeld einen eindeutigen Gerätenamen ein. Dieser Namen dient Ihnen zur Orientierung, welches der beiden Systeme zur Zeit im Normal-Modus läuft. Der Gerätenamen kann maximal 11 Zeichen lang sein.

   Encryption Key: Tragen Sie in das Eingabefeld ein Passwort ein.

   Sicherheitshinweis:

   Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35$4.

   Network Interface Card: Wählen Sie für die Datentransfer-Verbindung eine Netzwerkkarte aus. Diese Netzwerkkarte kann später nicht mehr konfiguriert werden.

   Wichtiger Hinweis:

   Die Netzwerkkarten müssen auf beiden Systemen die gleiche **Sys ID** haben (z. B. eth 3).
   Für die Überwachung mittels Heart-Beat-Anfrage wählen Sie in diesem Auswahlfeld bei beiden Systemen (Normal-Modus und Hot-Standby-Modus) eine Netzwerkkarte aus, die Link Beat unterstützt.

   Transfer Network: Tragen Sie in das Eingabefeld die **Netzwerk-Adresse** der Datentransfer-Verbindung ein.

Hinweis:

Für die Datentransfer-Verbindung kann nur ein Class-C-Netzwerk – Netzwerkmaske 255.255.255.0 - verwendet werden. Die Bit-Masken-Darstellung kann hier nicht verwendet werden.
Das für den Datenaustausch definierte Netzwerk darf nirgends sonst verwendet werden.

Das Eingabefeld enthält vom Internet-Sicherheitssystem generierte Vorschläge. Diese Vorschläge müssen von Ihnen nicht übernommen werden.

Serial Interface (OPTIONAL): Zusätzlich zur Datentransfer-Verbindung kann die Überwachung des aktiven Systems durch das Hot-Standby-System über die serielle Schnittstelle erfolgen. Über diese Verbindung erfolgt kein Datenaustausch. Wählen Sie im Drop-down-Menü die entsprechende serielle Schnittstelle aus.

Hinweis:

Wenn Sie nun die Eingaben wie nachfolgend beschrieben speichern, wird das System im Anschluss heruntergefahren und sofort wieder gestartet.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

   Das System 1 wird nun neu gebootet. Falls eine Tastatur angeschlossen ist, blinkt auf dem Keyboard die LED-Anzeige **Num**.

   Sobald das System den Hot-Standby-Modus erreicht, ertönen kurz hintereinander zwei Beeps und die LED-Anzeige hört auf zu blinken. Da das System 2 noch ausgeschaltet ist, bootet das System 1 weiter in den Normal-Modus und die LED-Anzeige **Num** blinkt wieder.

   Nachdem das System 1 den Bootvorgang abgeschlossen hat, hört die LED-Anzeige **Num** auf zu blinken und es ertönen im Sekundentakt fünf Beeps: Die MiddleWare hat nun alle Services, Regeln und Prozesse initialisiert.

Hinweis:

Falls die Signaltöne nicht ertönen und die LED-Anzeige noch blinkt, konnte die MiddleWare nicht alle Dienste, Regeln und Prozesse initialisieren. Wenden Sie sich in diesem Fall an den Support Ihres Sicherheitssystem-Anbieters.

Firewall-System 2 (Hot-Standby-Modus) konfigurieren:

8. Starten Sie das System 2.

9. Führen Sie auch hier die Schritte 3 bis 6 durch und klicken Sie anschließend zur Bestätigung auf die Schaltfläche **Save**.

   Das System 2 wird nun neu gebootet. Falls eine Tastatur angeschlossen ist, blinkt auf dem Keyboard die LED-Anzeige **Num**.

   Sobald das System den Hot-Standby-Modus erreicht, ertönen kurz hintereinander zwei Beeps und die LED-Anzeige hört auf zu blinken. Das System 2 erkennt über die Datentransfer-Leitung das aktive System 1 und verbleibt im Hot-Standby-Modus.

Das **High Availability**-System ist nun aktiv.

Über die Datentransfer-Verbindung wird das Internet-Sicherheitssystem im Hot-Standby-Modus ständig aktualisiert. Sobald das aktive System wegen einem Hardware-Defekt ausfällt, fährt das zweite System automatisch in den Normal-Modus und übernimmt dessen Funktion.

5.1.9. Shut down/Restart

Mit **Restart** wird das Internet-Sicherheitssystem heruntergefahren und wieder gestartet. Der **Restart** kann je nach Hardware und Konfiguration bis zu 5 Minuten dauern.

Restart:

1. Öffnen Sie im Verzeichnis **System** das Menü **Shut down/ Restart**.
2. Wählen Sie im Drop-down-Menü **Select action** die Aktion **Restart** aus.
3. Bestätigen Sie Ihre Auswahl durch einen Klick auf die Schaltfläche **Start**.
4. Beantworten Sie die Frage **Do you really want to restart?** durch einen Klick auf die Schaltfläche **OK**.

Mit **Shut down** können Sie das Internet-Sicherheitssystem herunterfahren.

Für Applikationen ohne Bildschirm und/oder LCD-Display ist besonders interessant, dass nach dem das System heruntergefahren wurde ein akustisches Signal ertönt: Endlos-Beep mit einer Sekunde Pause.

Der Vorgang dauert je nach Hardware und Konfiguration bis zu 5 Minuten. Erst nachdem Sie das System heruntergefahren haben, zu erkennen an der **Power down**-Ausgabe, dürfen Sie es ausschalten. Wenn das System, vor dem Ausschalten, nicht ordnungsgemäß heruntergefahren wurde, muss beim nächsten Startvorgang die Integrität des Filesystems überprüft werden – dies verzögert den Startvorgang. Im schlimmsten Fall können sogar Daten verloren gehen.
Wenn der Startvorgang erfolgreich war, ertönt ein akustisches Signal: Fünf Beeps in Folge.

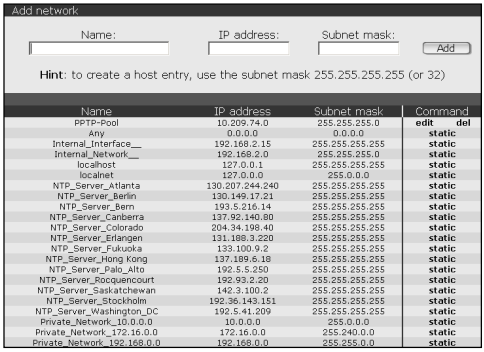
Shut down:

1. Öffnen Sie im Verzeichnis **System** das Menü **Shut down/ Restart**.
2. Wählen Sie im Drop-down-Menü **Select action** die Aktion **Shut down** aus.
3. Bestätigen Sie Ihre Auswahl durch einen Klick auf die Schaltfläche **Start**.
4. Beantworten Sie die Frage **Do you really want to shut down?** durch einen Klick auf die Schaltfläche **OK**.

5.2. Netzwerke und Dienste (Definitions)

Netzwerke und Dienste werden im Verzeichnis **Definitions** für alle weiteren Einstellungen, z. B. Paketfilter, VPN und Proxies zentral definiert. Dies hat den Vorteil, dass Sie später einfach mit den jeweiligen Bezeichnungen (**Name**) arbeiten können. Für eine weitere Vereinfachung sorgt die Möglichkeit, Netzwerke und Dienste zu gruppieren. Wenn Sie später diesen Gruppen bestimmte Einstellungen zuweisen, gelten diese für alle darin enthaltenen Netzwerke und Dienste. Gruppen können auch wieder in übergeordnete Gruppen zusammengefasst werden.
Außerdem definieren Sie in diesem Verzeichnis die lokalen Benutzer für die Proxydienste.

5.2.1. Networks



Name	IP address	Subnet mask	Command
PPTP-Pool	10.209.74.0	255.255.255.0	edit del
Any	0.0.0.0	0.0.0.0	static
Internal_Interface__	192.168.2.15	255.255.255.255	static
Internal_Network__	192.168.2.0	255.255.255.0	static
localhost	127.0.0.1	255.255.255.255	static
localnet	127.0.0.0	255.0.0.0	static
NTP_Server_Atlanta	130.207.244.240	255.255.255.255	static
NTP_Server_Berlin	130.149.17.21	255.255.255.255	static
NTP_Server_Bern	193.5.216.14	255.255.255.255	static
NTP_Server_Canberra	137.92.140.80	255.255.255.255	static
NTP_Server_Colorado	204.34.198.40	255.255.255.255	static
NTP_Server_Erlangen	131.188.3.220	255.255.255.255	static
NTP_Server_Fukuoka	133.100.9.2	255.255.255.255	static
NTP_Server_Hong Kong	137.189.6.18	255.255.255.255	static
NTP_Server_Palo_Alto	192.5.5.250	255.255.255.255	static
NTP_Server_Rocquencourt	192.93.2.20	255.255.255.255	static
NTP_Server_Saskatchewan	142.3.100.2	255.255.255.255	static
NTP_Server_Stockholm	192.36.143.151	255.255.255.255	static
NTP_Server_Washington_DC	192.5.41.209	255.255.255.255	static
Private_Network_10.0.0.0	10.0.0.0	255.0.0.0	static
Private_Network_172.16.0.0	172.16.0.0	255.240.0.0	static
Private_Network_192.168.0.0	192.168.0.0	255.255.0.0	static

Im Fenster **Add network** können Sie ein neues Netzwerk hinzufügen. Ein Netzwerk setzt sich immer aus **Namen**, **IP-Adresse** und **Netzwerkmaske** zusammen.

In der Netzwerk-Tabelle befinden sich bereits statisch eingetragene Netzwerke. Diese statischen Netzwerke vereinfachen den Support und können von Ihnen nicht editiert oder gelöscht werden.

Netzwerk hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Tragen Sie im Fenster **Add Network** in das Eingabefeld **Name** einen eindeutigen Netzwerknamen ein.
   Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

3. Tragen Sie in das Eingabefeld **IP address** die Adresse des Netzwerks ein.

4. Tragen Sie in das Eingabefeld **Subnet mask** die Netzwerkmaske ein.

   Beispiel: Sie können für ein Class-C Netzwerk die 255.255.255.0 eintragen oder die Bit-Masken-Darstellung verwenden. Für ein Class-C Netzwerk ist es 24.

5. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

WebAdmin prüft nun Ihre Eingaben auf semantische Gültigkeit.

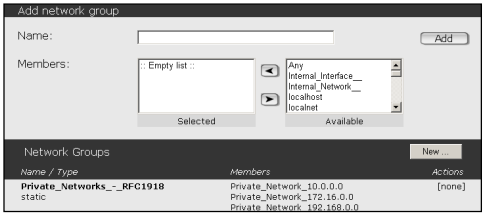
Nach erfolgreicher Definition wird das neue **Netzwerk** in die Netzwerk-Tabelle eingetragen. Sie finden dieses Netzwerk jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.
Für dieses Netzwerk können Sie z. B. unter **System/Settings** jetzt **WebAdmin** freischalten. Anschließend stehen Ihnen in der Spalte **Command** weitere Funktionen zur Verfügung.

Weitere Funktionen

Netzwerk editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Eingabemenü geladen. Anschließend können Sie die Eingaben bearbeiten.

Netzwerk löschen: Durch einen Klick auf die Schaltfläche **del** wird das Netzwerk aus der Tabelle gelöscht.

5.2.2. Network Groups



Netzwerke lassen sich zu Netzwerkgruppen zusammenfassen. Netzwerkgruppen werden behandelt wie einzelne Netzwerke und können wieder Teil einer übergeordneten Netzwerkgruppe sein.

Sie erkennen Netzwerkgruppen später daran, dass ihre Namen in geschweiften Klammern dargestellt werden. Alle auf dem

Internet-Sicherheitssystem definierten Netzwerkgruppen werden in der Tabelle **Network Groups** angezeigt.

Hinweis:

Jede Änderung in **Network Groups** wird ohne eine weitere Meldung sofort wirksam.

Netzwerkgruppe definieren:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Network Groups**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Network Group** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** einen eindeutigen Namen für die Netzwerkgruppe ein.
   Diesen Namen geben Sie später an, um z. B. Paketfilterregeln zu setzen.
4. Wählen Sie im Auswahlfeld **Members** die Netzwerke aus.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.
5. Bestätigen Sie nun Ihre Eingabe durch einen Klick auf die Schaltfläche **Add**.

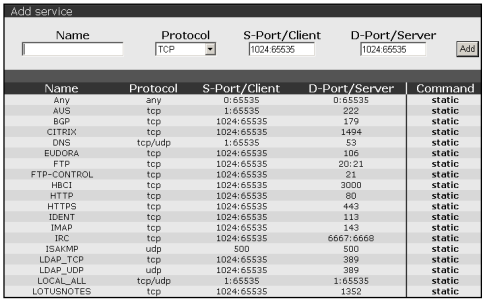
Nach erfolgreicher Definition wird die neue **Netzwerkgruppe** in die Tabelle **Network Groups** eingetragen. Sie finden diese Netzwerkgruppe jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Weitere Funktionen

Netzwerkgruppe editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Menü geladen. Anschließend können Sie der Netzwerkgruppe weitere Netzwerke hinzufügen oder einzelne Netzwerke aus der Gruppe entfernen.

Netzwerkgruppe löschen: Durch einen Klick auf die Schaltfläche **delete** wird die gesamte Netzwerkgruppe aus der Tabelle gelöscht.

5.2.3. Services



Name	Protocol	S-Port/Client	D-Port/Server	Command
Any	any	0:65535	0:65535	static
AUS	tcp	1:65535	222	static
BGP	tcp	1024:65535	179	static
CITRIX	tcp	1024:65535	1494	static
DNS	tcp/udp	1:65535	53	static
EUDORA	tcp	1024:65535	106	static
FTP	tcp	1024:65535	20:21	static
FTP-CONTROL	tcp	1024:65535	21	static
HBCI	tcp	1024:65535	3000	static
HTTP	tcp	1024:65535	80	static
HTTPS	tcp	1024:65535	443	static
IDENT	tcp	1024:65535	113	static
IMAP	tcp	1024:65535	143	static
IRC	tcp	1024:65535	6667:6668	static
ISAKMP	udp	500	500	static
LDAP_TCP	tcp	1024:65535	389	static
LDAP_UDP	udp	1024:65535	389	static
LOCAL_ALL	tcp/udp	1:65535	1:65535	static
LOTUSNOTES	tcp	1024:65535	1352	static

Dienste (Services) sind Definitionen für den Datenverkehr über Netzwerke, z. B. das Internet. Eine Dienstedefinition besteht aus **Namen**, **Protokollen** und **Ports**.

Folgende Protokolle stehen Ihnen zur Verfügung: TCP, UDP, TCP und UDP, ICMP, AH und ESP.

UDP verwendet Ports von 0 bis einschließlich 65535 und ist ein Protokoll, das kein sog. ACK-Bit benötigt. UDP arbeitet besonders beim Versenden kleinerer Datenmengen schneller als **TCP**. Verlorene Pakete können über **UDP** nicht erkannt und neu angefordert werden, da es sich um ein verbindungsloses Protokoll handelt. Der Erhalt der Datenpakete wird vom Empfänger nicht quittiert.

TCP-Verbindungen benutzen ebenfalls die Ports von 0 bis 65535. Verlorene Pakete können über **TCP** erkannt und neu angefordert werden. Bei **TCP** werden alle Datenpakete vom Empfänger quittiert (verbindungsorientiertes Protokoll). Eine **TCP**-Verbindung wird zu Beginn mit dem sog. **Three Way Handshake**-Verfahren aufgebaut und nach dem Transfer wieder abgebaut.

Die Protokolle **AH** und **ESP** werden für **Virtual Private Network** (**VPN**) benötigt. Diese Protokolle werden im Kapitel 5.6 ab Seite 209 beschrieben.

Dienst hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Service**.
2. Tragen Sie in das Eingabefeld **Name** einen eindeutigen Namen für den **Dienst (Service)** ein.
   Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen.
3. Wählen Sie im Drop-down-Menü **Protocol** das **Protokoll** aus.

4. Die Einstellungen richten sich nun nach dem ausgewählten Protokoll.

   Für die Protokolle **TCP** und **UDP** benötigen Sie die folgenden zwei Werte. Eingabe-Optionen: Einen einzelnen Port (z. B. 80) oder eine Portrange (z. B. 1024:64000).

   S-Port/Client: Tragen Sie hier den Source-Port, d. h. die Client-Seite des Dienstes ein.

   D-Port/Server: Legen Sie hier den Destination-Port, d. h. die Server-Seite des Dienstes fest.

   Die Protokolle **AH** und **ESP** werden für **IPSec VPN**-Verbindungen benötigt. Der hier eingetragene Wert muss zuvor mit der Gegenstelle des IPSec VPN-Tunnels abgesprochen werden.

   SPI: Tragen Sie hier einen Wert zwischen 256 und 65535 ein. Die Werte bis einschließlich 255 sind vom **Internet Assigned Numbers Authority (IANA)** reserviert.

   Für das Protokoll **ICMP** können Sie im Auswahlmenü **ICMP type** die enthaltene Nachricht auswählen.

5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

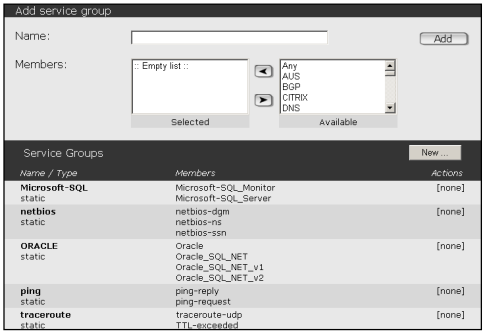
Nach erfolgreicher Definition wird der neue **Dienst (Service)** in eine der Dienstetabelle eingetragen. Anschließend stehen Ihnen in der Spalte **Command** weitere Funktionen zur Verfügung.

Weitere Funktionen

Dienst editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Eingabemenü geladen. Anschließend können Sie die Eingaben bearbeiten.

Dienst löschen: Durch einen Klick auf die Schaltfläche **del** wird der Dienst aus der Tabelle gelöscht.

5.2.4. Service Groups



Dienste lassen sich zu **Dienstgruppen (Service Groups)** zusammenfassen. Dienstgruppen werden behandelt wie einzelne Dienste und können wieder Teil einer übergeordneten Dienstgruppe sein.
Sie erkennen eine Dienstgruppe später daran, dass ihr Name in geschweiften Klammern dargestellt wird.

Hinweis:

Jede Änderung in **Service Groups** wird ohne eine weitere Meldung sofort wirksam!

Dienstgruppe definieren:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Service Groups**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Service Group** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** einen eindeutigen Namen für die Dienstgruppe ein.
   Diesen Namen geben Sie später an, um z. B. übergeordnete Dienstgruppen zu erstellen oder Paketfilterregeln zu setzen.
4. Wählen Sie im Auswahlfeld **Members** die Netzwerke aus.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.
5. Bestätigen Sie nun Ihre Eingabe durch einen Klick auf die Schaltfläche **Add**.

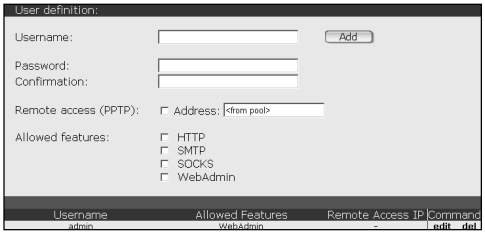
Nach erfolgreicher Definition wird die neue **Dienstgruppe** in die Tabelle **Service Groups** eingetragen. Sie finden diese Dienstgruppe jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Weitere Funktionen

Dienstgruppe editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Menü geladen. Anschließend können Sie der Dienstgruppe weitere Dienste hinzufügen oder einzelne Dienste aus der Gruppe entfernen.

Dienstgruppe löschen: Durch einen Klick auf die Schaltfläche **delete** wird die gesamte Dienstgruppe aus der Tabelle gelöscht.

5.2.5. Users



In diesem Menü werden lokale **Benutzer (Users)** hinzugefügt, wenn der Gebrauch der Proxydienste nach Personen eingeschränkt werden soll. Dies ist die Alternative dazu, eine externe User-Datenbank abzufragen. Hier legen Sie fest, auf welche Proxydienste ein Benutzer Zugriff hat. Mögliche Optionen sind PPTP (Remote Access), HTTP-Proxy, SMTP-Proxy, SOCKS-Proxy und WebAdmin.

Sicherheitshinweis:

Standardmäßig hat nur der **admin**-Benutzer Zugriff auf das Konfigurationstool **WebAdmin**.
Sie sollten das Passwort zum Konfigurationstool in regelmäßigen Abständen ändern.

Benutzer hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Users**.
2. Tragen Sie im Eingabefeld **Username** den Namen des Benutzers ein.
3. Tragen Sie im Eingabefeld **Password** das Passwort ein und bestätigen es nochmals im Eingabefeld **Confirmation**.

Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35$4.

4. Wenn der Benutzer sich über **PPTP** in Ihrem Netzwerk anmelden soll, aktivieren sie die Option **Remote access (PPTP)**. Wenn dem Benutzer bei der Anmeldung eine bestimmte IP-Adresse zugewiesen werden soll, tragen Sie diese in das Eingabefeld **Address** ein.
   Weitere Informationen zu **PPTP Roadwarrior Access** finden Sie im Kapitel 5.3.6 ab Seite 148.

5. Legen Sie nun durch einen Klick auf die Optionsfelder fest, auf welche Dienste der Benutzer Zugriff hat.
   Eingabe-Optionen: HTTP-Proxy, SMTP-Proxy, SOCKS-Proxy und WebAdmin.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Nach erfolgreicher Definition wird der neue Benutzer in die Benutzer-Tabelle eingetragen. Anschließend stehen Ihnen in der Spalte **Command** weitere Funktionen zur Verfügung.

Weitere Funktionen

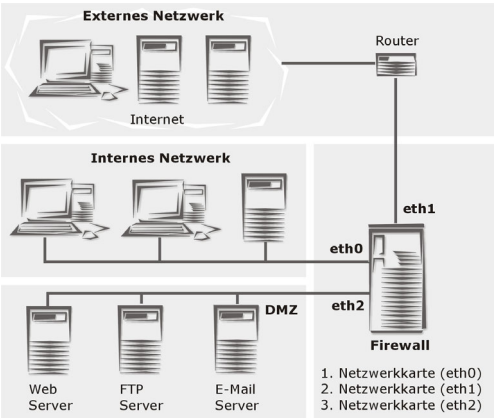
Benutzer editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Menü geladen. Anschließend können Sie die Eingaben bearbeiten.

Benutzer löschen: Durch einen Klick auf die Schaltfläche **del** wird der Benutzer aus der Tabelle gelöscht.

5.3. Netzwerkeinstellungen (Network)

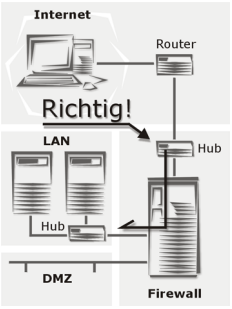
Im Verzeichnis **Network** konfigurieren Sie die Netzwerkkarten und virtuellen Schnittstellen (**Interfaces**) und führen netzwerkspezifische Einstellungen durch.

5.3.1. Interfaces

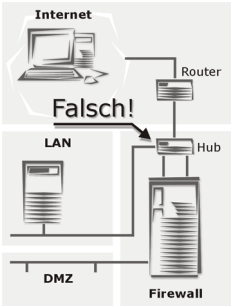


Um ein internes Netzwerk (LAN) vor einem externen Netzwerk (Internet) zu sichern, benötigt eine Firewall mindestens zwei **Netzwerkkarten**. In unseren Beispielen ist die **Netzwerkkarte eth0** immer die Schnittstelle zum internen Netzwerk. Die **Netzwerkkarte eth1** ist die Schnittstelle zum externen Netzwerk (Internet). Diese beiden Seiten werden auch **Trusted** und **Untrusted** genannt.

Während der Installation werden die Netzwerkkarten automatisch erkannt. Falls später weitere Netzwerkkarten hinzugefügt werden, ist eine Neu-Installation des Internet-Sicherheitssystems notwendig. Verwenden Sie die Backup-Funktion, um nach der Neu-Installation Ihre alte System-Konfiguration wieder einzuspielen.



Die Firewall muss, wie in der linken Grafik dargestellt, die Schnittstelle zwischen dem LAN und dem Internet sein. Alle Datenpakete müssen das Internet-Sicherheitssystem passieren.



Wir raten dringend davon ab, die Schnittstellen der Firewall, wie in der rechten Grafik dargestellt, über einen Hub oder Switch physikalisch zusammen auf ein Netzwerksegment zu legen, wenn dieser nicht als VLAN-Switch konfiguriert ist. Unter Umständen kann es dann zu falschen ARP-Auflösungen (Address Resolution Protocol) kommen (ARP-Clash), die nicht alle Betriebssysteme (z. B. die von Microsoft) verwalten können. Pro Firewall-Netzwerk-Schnittstelle muss daher auch ein physikalisches Netzwerk-Segment verwendet werden.

Im Menü **Interfaces** verwalten Sie alle auf dem Internet-Sicherheitssystem installierten Netzwerkkarten und konfigurieren die Schnittstelle zum externen Netzwerk (Internet) sowie die Schnittstellen zu den internen Netzwerken (LAN, DMZ).

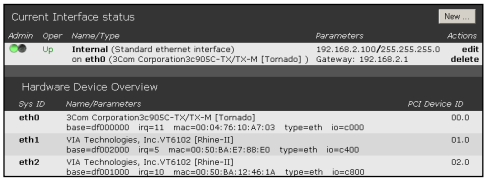
Hinweis:

Beachten Sie bei der Planung und Konfiguration der Schnittstellen, welche Netzwerkkarten Sie jeweils auf dem Sicherheitssystem auswählen. Für die Schnittstelle zum externen Netzwerk (Internet) wird in der Regel die Netzwerkkarte mit der Sys ID **eth1** verwendet.

Für eine spätere Installation des **High Availability (HA)**-Systems benötigen Sie auf beiden Systemen eine Netzwerkkarte mit gleicher Sys ID. Die Installation des **HA**-Systems wird in Kapitel 5.1.8 ab Seite 89 beschrieben.

In den nachfolgenden Abschnitten wird erklärt, wie die verschiedenen Schnittstellen-Typen (**Interface Types**) über die Fenster **Current Interface Status** und **Hardware Device Overview** verwaltet und konfiguriert werden.

Current Interface Status


Current Interface status
New ...
Admin Oper Name/Type Parameters Actions
Up Internal (Standard ethernet interface) on eth0 (3Com Corporation3c905C-TX/TX-M [Tornado]) 192.168.2.100/255.255.255.0 Gateway: 192.168.2.1 edit delete
Hardware Device Overview
Sys ID Name/Parameters PCI Device ID
eth0 3Com Corporation3c905C-TX/TX-M [Tornado] base=df000000 irq=11 mac=00:04:76:10:A7:03 type=eth io=c000 00.0
eth1 VIA Technologies, Inc.VT6102 [Rhine-II] base=df002000 irq=5 mac=00:50:BA:E7:88:E0 type=eth io=c400 01.0
eth2 VIA Technologies, Inc.VT6102 [Rhine-II] base=df001000 irq=10 mac=00:50:BA:12:46:1A type=eth io=c800 02.0

In diesem Fenster konfigurieren Sie die Netzwerkkarten und virtuellen Schnittstellen (**Interfaces**). In der Tabelle werden alle bereits konfigurierten Netzwerkarten angezeigt. Das linke Bild zeigt das Menü **Interfaces** nach der Installation der Software mit drei eingebauten Ethernet-Netzwerkkarten.

Während der Installation wurde die Schnittstelle mit der Bezeichnung **eth0** bereits konfiguriert. Sie ist die Schnittstelle zwischen dem Internet-Sicherheitssystem und dem internen Netzwerk (LAN). Per Default wird dieser Netzwerkkarte der Namen **Internal** zugewiesen.
In der Tabelle sind alle Informationen zu den konfigurierten Schnittstellen enthalten: Schnittstelle ein/aus (Statusampel zeigt **Grün**/**Rot**), der aktuelle Funktionszustand (**Up**/**Down**), Name (**Name**), Bezeichnung (**Sys ID**) und Netzwerkkarten-Typ (**eth**/**wlan**) sowie IP-Adresse und Netzwerkmaske (**Parameters**).
Durch einen Klick auf die Statusampel in der Spalte **Admin** wird die Schnittstelle ein- und ausgeschaltet. Mit den Funktionen in der Spalte **Actions** können Sie die Schnittstellen bearbeiten (**edit**) oder entfernen (**delete**).

Bei diesem Internet-Sicherheitssystem weisen Sie jeder virtuellen Schnittstelle einen **Namen** und eine bestimmte Netzwerkkarte zu. Für jede konfigurierte Schnittstelle werden anschließend automatisch drei logische Netzwerke definiert:

- Eine Schnittstelle (**NAME_Interface__**), bestehend aus der von Ihnen definierten IP-Adresse und der Netzwerkmaske 255.255.255.255 (Host)
- Ein Netzwerk (**NAME_Network__**), bestehend aus der Netzwerk-IP-Adresse und der Netzwerkmaske (Netzwerk)
- Broadcast (**NAME_Broadcast__**), bestehend aus der Broadcast-IP und der Netzwerkmaske 255.255.255.255 (Host)

Die Netzwerken werden im Menü **Networks** angezeigt. Wenn bei einer Netzwerkkarte eine dynamische IP-Adressenverteilung, z. B. bei **DHCP** oder **PPPoE** verwendet wird, werden diese Einstellungen automatisch aktualisiert. Alle Funktionen die sich auf

diese Einstellungen beziehen (z. B. Paketfilter oder NAT), erhalten automatisch die geänderte IP-Adresse.

Hardware Device Overview

In dieser Tabelle sind alle auf dem Internet-Sicherheitssystem installierten Netzwerkkarten mit den entsprechenden Hardware-Informationen enthalten, z. B. die vom System zugewiesene Bezeichnung (**Sys ID**), der Netzwerkarten-Typ, die MAC-Hardware-Adresse (**Name/Parameters**) sowie Angaben zum PCI-Bus: Bus/Gerät/Funktion (**PCI Device ID**).

Fehler: In der Tabelle **Hardware Device overview** sind nicht alle Netzwerkkarten enthalten.

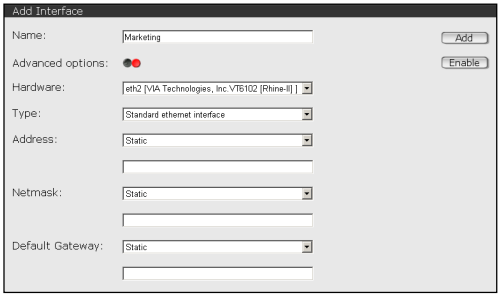
Mögliche Fehlerursache:

Die fehlende Netzwerkkarte wurde erst nach Installation des Internet-Sicherheitssystems eingebaut oder sie wurde während der Installation nicht erkannt.
Setzen Sie sich in diesem Fall mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

Achtung:

Wenn Sie die **IP-Adresse** der internen Netzwerkkarte **eth0** ändern, besteht die Möglichkeit, dass Sie sich "aussperren".

5.3.1.1. Standard Ethernet Interface



Für eine Standard-Ethernet-Schnittstelle zu einem internen oder externen Netzwerk muss auf der Netzwerkkarte die primäre Netzwerkkarten-Adresse eingerichtet werden.

Alle auf dem Internet-Sicherheitssystem installierten Netzwerkkarten werden in der Tabelle **Hardware Device Overview** angezeigt.

Standard-Ethernet-Netzwerkkarte einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

   Tipp:

   Wählen Sie als Schnittstelle zum externen Netzwerk (Internet) die Netzwerkkarte mit der Sys ID **eth1** aus.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Standard ethernet interface** aus.

   Beachten Sie, dass einer Netzwerkkarte nicht gleichzeitig der Typ **Standard ethernet interface** und **PPP over Ethernet (PPPoE-DSL) connection** oder **PPPTP over Ethernet (PPPoA-DSL) connection** zugewiesen werden kann.

6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ durch:

Address: Falls Sie eine statische IP-Adresse eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

Netmask: Falls Sie eine statische Netzwerkmaske eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Netzwerkmaske ein. Wenn Sie die Netzwerkmaske durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

Default Gateway: Bei einem statischen Default Gateway wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

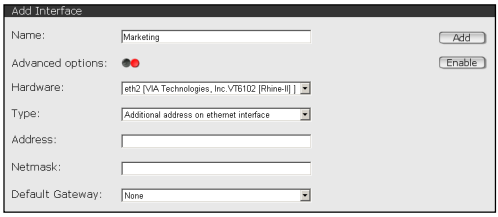
Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Advanced Options

Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für die erweiterten Funktionen geöffnet.

Die erweiterten Funktion (**Advanced Options**) werden für alle Schnittstellen-Typen im Kapitel 5.3.1.7 ab Seite 131 beschrieben.

5.3.1.2. Additional address on ethernet interface



Einer Netzwerkkarte können mehrere zusätzliche IP-Adressen zugeordnet werden (IP-Aliase). Diese Funktion wird benötigt, um auf einer Netzwerkkarte mehrere logische Netzwerke zu verwalten. Sie kann auch im Zusammenhang mit der Funktion **NAT** notwendig sein, um dem Internet-Sicherheitssystem zusätzliche Adressen zuzuweisen. Die Funktion **NAT** wird in Kapitel 5.3.3 ab Seite 134 beschrieben. Auf jeder Netzwerkkarte können bis zu 255 zusätzliche Adressen konfiguriert werden.

Zusätzliche Adresse einer Netzwerkkarte zuweisen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Additional address on ethernet interface** aus.
6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ durch.

   Address: Bei diesem Schnittstellen-Type kann nur eine statische IP-Adresse gesetzt werden. Tragen Sie in das Eingabefeld die Adresse ein.

Netmask: Bei diesem Schnittstellen-Type kann nur eine statische Netzwerkmaske gesetzt werden. Tragen Sie in das Eingabefeld die Netzwerkmaske ein.

Default Gateway: Wenn Sie ein Default Gateway definieren möchten wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

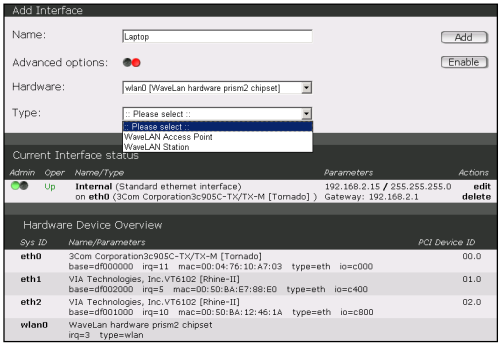
8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Advanced Options

Für diesen Schnittstellen-Typ können keine erweiterten Funktionen (**Advanced Options**) eingestellt werden.

5.3.1.3. Wireless LAN



Für **Wireless LAN** gelten die Standards der Gruppe IEEE 802.11. Das Internet-Sicherheitssystem unterstützt die Variante **IEEE 802.11b**. Dieser Standard arbeitet auf dem Funkfrequenzband 2,4 GHz und liegt im **ISM**-Frequenzbereich. **ISM** steht für **Industrial Scientific and Medical**. Diese ISM-Frequenzen können von der Industrie, der Wissenschaft und der Medizin lizenzfrei genutzt werden, d. h. für die Nutzung dieser Frequenzen auf privatem Grund und Boden müssen keine Gebühren bezahlt werden. Der Standard IEEE 802.11b ermöglicht eine maximale Bandbreite von 11 Mbit/s. Für die Planung des Wireless LAN muss noch beachtet werden, dass die Bandbreite abnimmt, je größer die zu überbrückende Reichweite ist.

Wichtiger Hinweis:

zur Konfiguration einer Schnittstelle zum **Wireless LAN** benötigen Sie eine **PCMCIA-Karte** mit kompatiblem **Prism2**-Chipsatz. Die vom Internet-Sicherheitssystem unterstützte Hardware ist unter der Internetadresse **http://docs.astaro.org** im Verzeichnis **Hardware Compatibility List for Astaro Security Linux** aufgelistet.

Die Schnittstelle zwischen Internet-Sicherheitssystem und Wireless LAN kann als **Wireless LAN Access Point** oder **Wireless LAN Station** konfiguriert werden.

Mit **Wireless LAN Access Point** werden die drahtlos vernetzten Rechner (Clients) über diese Schnittstelle miteinander verbunden. Die Funktion entspricht einem Hub im verdrahteten Netzwerk. Über das Internet-Sicherheitssystem kann das drahtlose Netzwerk anschließend an das kabelbasierte LAN angebunden werden.

Mit **Wireless LAN Station** wird das Internet-Sicherheitssystem an ein bestehendes drahtloses Netzwerk angemeldet und

fungiert als einfacher Endpunkt. Nur bei diesem Wireless LAN-Schnittstellen-Typ können Sie die Adressen auch durch einen DHCP-Server zuweisen lassen.

Wireless LAN Security

Für die Verschlüsselung des Wireless LAN sieht der Standard 802.11 das Verschlüsselungsverfahren **WEP** vor. WEP ist die Abkürzung für **Wired Equivalent Privacy**. Dieses Verschlüsselungsverfahren basiert auf der RC4-Chiffrierung, wobei ein Schlüssel für die Kodierung und Dekodierung verwendet wird. Bei Aktivierung der WEP-Verschlüsselung wird ein geheimer Schlüssel erstellt, der auf allen Wireless-LAN-Schnittstellen, die zu diesem Funknetzwerk gehören, gleich konfiguriert sein muss. Wenn nun eine Datenübertragung zwischen zwei mobilen Rechnern stattfindet, werden die Daten zunächst mit Hilfe des geheimen Schlüssels chiffriert und anschließend an den Zielrechner übertragen. Dort werden die Daten mit Hilfe des gleichen Schlüssels wieder dekodiert. Wer nicht über den korrekten Schlüssel verfügt, kann die Daten nicht dechiffrieren.

Bei diesem Internet-Sicherheitssystem kann **WEP** auch zur **Authentifizierung** genutzt werden. Wenn ein Rechner dem Wireless LAN beitreten will, aber nicht über den passenden Schlüssel verfügt, wird die Verbindung seitens des Access-Points getrennt.

Beim Schnittstellen-Typ **Wireless LAN Access Point** können Sie für **Stations** den Zugang in das Wireless LAN durch **Filtern der MAC-Adressen** kontrollieren. Generell läßt sich ein Wireless LAN recht flexibel erweitern, doch sollte immer noch der Netzwerk-Administrator entscheiden dürfen, wann und welcher Rechner eingebunden werden soll. Wenn Sie nun einen solchen Filter definieren, dann legen Sie z. B. fest, dass der Rechner mit der MAC-Adresse 00:04:76:26:65:4C dem Wireless LAN beitreten darf, alle anderen Rechner werden ausgeschlossen. Sobald nun ein Rechner diesem Wireless LAN beitreten möchte, wird die MAC-Adresse der Netzwerkkarte überprüft. Falls diese MAC-Adresse in der Zugriffskontrollliste enthalten ist, kann die Funkverbindung zum Wireless LAN erfolgen, andernfalls ist keine funkbasierte Verbindung möglich.

Bei diesem Internet-Sicherheitssystem haben Sie die Möglichkeit einen **negativen** oder einen **positiven MAC-Adressen-Filter** zu konfigurieren. Beim **negativen Filter** sind grundsätzlich alle

MAC-Adressen zugelassen. Sie definieren in einer Zugriffskontrollliste nur die Netzwerkkarten, die das Wireless LAN nicht betreten dürfen.
Beim **positiven Filter** werden zuerst alle MAC-Adressen ausgeschlossen. Sie müssen in einer Zugriffskontrollliste explizit angeben, welche Netzwerkkarten das Wireless LAN betreten dürfen.
Wenn Sie die Wahl haben, dann sollten Sie den weitaus sicheren positiven Filter verwenden.

Für die Konfiguration der Wireless LAN-PCMCIA-Karte benötigen Sie die folgenden Daten:

- **SSID**: Die Abkürzung steht für **Service Set Identifier** und ist der Name des Funknetzwerks. Ein Wireless LAN kann aus mehreren Funknetzwerken mit unterschiedlichen Funkkanälen bestehen. Den Namen eines Funknetzwerks kann man relativ frei wählen. Bei diesem System ist es eine beliebige Zeichenkette ohne Leerzeichen.
  Falls Sie den Schnittstellen-Typ **Wireless LAN Station** konfigurieren, um den Zugang zu einem bereits vorhanden Funknetzwerk zu erhalten, benötigen Sie den bestehenden Namen. Der Namen kann eine maximale Länge von 32 Zeichen haben.
- **Channel**: Bei diesem System geben Sie den Funkkanal des Funknetzwerks manuell ein. Sollten noch weitere Funknetzwerke vorhanden sein, vergewissern Sie sich, welche Kanäle von diesen belegt werden.
  Beachten Sie außerdem, dass in verschiedenen Ländern nur bestimmte Kanäle verwendet werden dürfen:

Land	Kanal
USA & Kanada	1 bis 11
Europa (ETSI)	1 bis 14
Japan	1 bis 14

Land	Kanal
Spanien	10/11
Frankreich	10 bis 13

- **WEP**: Für die WEP-Verschlüsselung benötigen Sie mindestens einen WEP-Schlüssel. Maximal vier Schlüssel sind möglich. Sie können eine Schlüssellänge von 40 Bit oder 104 Bit definieren. Je nachdem für welche Schlüssellänge Sie sich entscheiden, müssen Sie eine Zeichenfolge von 5 oder 13 Zeichenpaaren in hexadezimaler Schreibweise eingegeben. Sie dürfen also nur die Zahlen 0 bis 9 und die Buchstaben A bis F verwenden.
  Beispiel für einen 40-Bit-Schlüssel: 17:A5:6B:45:23

- **Access Mode** (nur Wireless LAN Access Point): Für den MAC-Adressen-Filter müssen Sie zuerst die MAC-Adressen der Netzwerkkarten zusammenstellen, die entweder das Wireless LAN nicht betreten dürfen (negativer Filter) oder das Wireless LAN explizit betreten dürfen (positiver Filter).
  Wie Sie die Netzwerkkarten-MAC-Adresse ermitteln wird nachfolgend erklärt.

Die MAC-Adressen ermitteln:

Falls die Netzwerkkarten noch nicht eingebaut sind, brauchen Sie die jeweilige MAC-Adresse nur noch zu notieren, da sich die Adresse auf der Netzwerkkarte befindet.

Wenn das Wireless LAN bereits in Betrieb ist und Sie den Filter nachträglich konfigurieren möchten, erhalten Sie die MAC-Adresse auch mit Hilfe der folgenden Kommandozeilenbefehle. Falls es sich um ein kleines Wireless LAN handelt und die mobilen Rechner in unmittelbarer Nähe stehen, gehen Sie folgendermaßen vor:

1. Öffnen Sie unter MS Windows die **Eingabeaufforderung**.

   Sie finden die **Eingabeaufforderung** in MS Windows unter **Start/Programme/Zubehör/Eingabeaufforderung**.

2. Geben Sie in der Kommandozeile den folgenden Befehl ein:

   ipconfig –all

3. Drücken Sie auf die **Enter**-Taste.

   In der Zeile **Physikalische Adresse** steht die MAC-Adresse, z. B. 00-04-76-26-65-4C.

4. Schließen Sie anschließend die Eingabeaufforderung.

Falls es sich bei Ihrem Netzwerk um ein größeres Netzwerk handelt, können Sie die MAC-Adressen auch mit Hilfe des Ping-Befehls ermitteln:

1. Stellen Sie sicher, dass der jeweilige Rechner angeschaltet und hochgefahren ist.

2. Öffnen Sie unter MS Windows die **Eingabeaufforderung**.

   Sie finden die Eingabeaufforderung in MS Windows unter **Start/Programme/Zubehör/Eingabeaufforderung**.

3. Pingen Sie den Zielrechner an, indem Sie folgenden Befehl eingeben:

   ping IP-Adresse, z. B. ping 192.168.2.15

4. Drücken Sie auf die **Enter**-Taste.

   Sofern der Zielrechner erreichbar ist, erhalten Sie eine Antwort.

5. Geben Sie den folgenden Befehl ein:

   arp –g

6. Drücken Sie auf die **Enter**-Taste.

   In Ihrer lokalen ARP-Tabelle befindet sich nun in der Spalte **Physikalische Adresse** die MAC-Adresse und die dazugehörige IP-Adresse.

Wenn Sie eine Netzwerkverbindung zu einem anderen Rechner herstellen möchten, erfolgt die Adressierung der Frames über die MAC-Adresse. Diese Adresse muss also bekannt sein, weshalb der Zielrechner einen ARP-Request erhält und zur Bekanntgabe der MAC-Adresse veranlasst wird. Der Quellrechner erhält daraufhin eine Antwort und die Informationen werden in der lokalen ARP-Tabelle abgelegt.

Wenn Sie nun die **PCMCIA-Karte** für das **Wireless LAN** als **Access Point** konfigurieren möchten, gehen Sie wie nachfolgend beschrieben vor. Die Konfiguration der PCMCIA-Karte als **Station** wird ab Seite 119 erklärt.

Wireless LAN Access Point einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.

2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.

3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.

4. Wählen Sie im Drop-down-Menü **Hardware** die **Wireless LAN**-Netzwerkkarte aus.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Wireless LAN Access Point** aus.

6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ **Wireless LAN Access Point** durch.

   Address: Weisen Sie dem Access-Point eine IP-Adresse zu. Bei diesem Schnittstellen-Type kann nur eine statische IP-Adresse gesetzt werden. Tragen Sie in das Eingabefeld die Adresse ein.

   Netmask: Bei diesem Schnittstellen-Type kann nur eine statische Netzwerkmaske gesetzt werden. Tragen Sie in das Eingabefeld die Netzwerkmaske ein.

   Default Gateway: Wenn Sie ein Default Gateway definieren möchten wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

   SSID: Tragen Sie in das Eingabefeld den Funkzellennamen ein. Geben Sie eine beliebige Zeichenkette ohne Leerzeichen ein. Die Zeichenkette kann maximal 32 Zeichen lang sein.

   Channel: Stellen Sie in diesem Drop-down-Menü den Frequenzkanal des Wireless LANs ein.

   Use WEP: Wenn Sie im Wireless LAN die WEP-Verschlüsselung verwenden möchten, wählen Sie im Drop-down-Menü **Yes** aus.

   Sicherheitshinweis:

   Die WEP-Verschlüsselung sollte immer verwendet werden, da ein ungeschütztes Wireless LAN immer ein hohes Sicherheitsrisiko darstellt.

   Wenn Sie die WEP-Verschlüsselung auf **No** stellen, werden die weiteren Einstellungen in den WEP-spezifischen Feldern vom System nicht mehr berücksichtigt.

   WEP Authentication: Falls WEP zur Authentifizierung eingesetzt werden soll, wählen Sie im Drop-down-Menü **Yes** aus. Dies hat zur Folge, dass dem Rechner im Wireless LAN der aktuelle **WEP Key** bekannt sein muss.

   Require WEP: Wenn Rechner, die die WEP-Verschlüsselung nicht unterstützen, keine Verbindung zum Wireless LAN erhalten sollen, wählen Sie **Yes** aus.

WEP Key: Tragen Sie in die Eingabefelder **WEP Key 0 bis 3** die WEP-Schlüssel ein. Für die Verschlüsselung benötigen Sie mindestens einen WEP-Schlüssel. Maximal vier Schlüssel sind möglich.

Für eine Schlüssellänge von 40 Bit geben Sie eine Zeichenkette mit 5 Zeichenpaaren ein. Für eine Schlüssellänge von 104 Bit benötigen Sie eine Zeichenkette mit 13 Zeichenpaaren. Die Zeichenfolge muss in hexadezimaler Schreibweise eingegeben werden. Sie dürfen also nur die Zahlen 0 bis 9 und die Buchstaben A bis F verwenden.
Beispiel für einen 40-Bit-Schlüssel: 17:A5:6B:45:23

Default WEP Key: Wählen Sie im Drop-down-Menü einen der WEP-Schlüssel 0 bis 3 (**WEP Key**) zum Default-Schlüssel aus. Dies ist der aktuelle WEP-Schlüssel, den die Rechner benötigen, um das Wireless LAN zu betreten.

Access Mode: Wählen Sie im Drop-down-Menü den Filter für das Wireless LAN aus. Wenn Sie allen Rechnern den Zutritt zum Wireless LAN erlauben möchten, wählen Sie **All stations can get access** aus.
Wenn Sie den **positiven Filter** konfigurieren möchten, wählen Sie **Stations in Allowed MAC addrs can get access** aus. Für den **negativen Filter** wählen Sie **Stations in Denied MAC addrs can not get access** aus.

Allowed MAC addrs: Wenn Sie zuvor den **positiven Filter** ausgewählt haben, tragen Sie in die Zugriffskontrollliste die MAC-Adressen der Rechner ein, die das Wireless LAN betreten dürfen.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Denied MAC addrs: Wenn Sie zuvor den **negativen Filter** ausgewählt haben, tragen Sie in die Zugriffskontrollliste die MAC-Adressen der Rechner ein, die das Wireless LAN nicht betreten dürfen.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Wireless LAN Station einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die **Wireless LAN**-Netzwerkkarte aus.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Wireless LAN Station** aus.
6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ **Wireless LAN Station** durch.

   Address: Weisen Sie der Station eine IP-Adresse zu. Falls Sie eine statische IP-Adresse eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Netmask: Falls Sie eine statische Netzwerkmaske eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Netzwerkmaske ein. Wenn Sie die Netzwerkmaske durch einen DHCP-Server zu-

weisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

Default Gateway: Bei einem statischen Default Gateway wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

SSID: Tragen Sie in das Eingabefeld den Funkzellennamen ein. Wenn Sie die Verbindung zu einem bereits bestehenden Wireless LAN aufbauen möchten, müssen Sie den bestehenden Funkzellennamen eintragen.

Use WEP: Wenn Sie im Wireless LAN die WEP-Verschlüsselung verwenden möchten, wählen Sie im Drop-down-Menü **Yes** aus.

Sicherheitshinweis:

Die WEP-Verschlüsselung sollte immer verwendet werden, da ein ungeschütztes Wireless LAN immer ein hohes Sicherheitsrisiko darstellt.

Wenn Sie die WEP-Verschlüsselung auf **No** stellen, werden die weiteren Einstellungen in den WEP-spezifischen Feldern vom System nicht mehr berücksichtigt.

WEP Authentication: Falls WEP zur Authentifizierung eingesetzt werden soll, wählen Sie im Drop-down-Menü **Yes** aus. Dies hat zur Folge, dass dem Rechner im Wireless LAN der aktuelle **WEP Key** bekannt sein muss.

Require WEP: Wenn Rechner, die die WEP-Verschlüsselung nicht unterstützen, keine Verbindung zum Wireless LAN erhalten sollen, wählen Sie **Yes** aus.

WEP Key: Tragen Sie in die Eingabefelder **WEP Key 0 bis 3** die WEP-Schlüssel ein. Für die Verschlüsselung benötigen Sie mindestens einen WEP-Schlüssel. Maximal vier Schlüssel sind möglich.

Für eine Schlüssellänge von 40 Bit geben Sie eine Zeichenkette mit 5 Zeichenpaaren ein. Für eine Schlüssellänge von 104 Bit benötigen Sie eine Zeichenkette mit 13 Zeichenpaaren. Die Zeichenfolge muss in hexadezimaler Schreibweise eingegeben werden. Sie dürfen also nur die Zahlen 0

bis 9 und die Buchstaben A bis F verwenden.
Beispiel für einen 40-Bit-Schlüssel: 17:A5:6B:45:23

Default WEP Key: Wählen Sie im Drop-down-Menü einen der WEP-Schlüssel 0 bis 3 (**WEP Key**) zum Default-Schlüssel aus. Dies ist der aktuelle WEP-Schlüssel, den die Rechner benötigen, um das Wireless LAN zu betreten.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

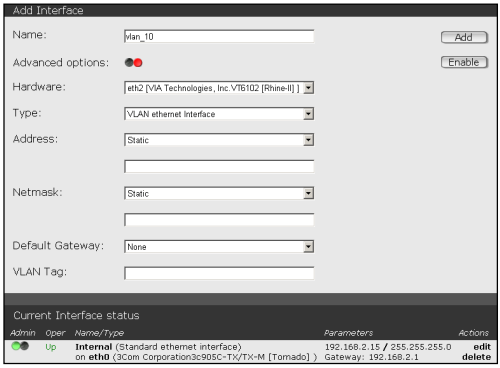
Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Advanced Options

Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für die erweiterten Funktionen geöffnet.

Die erweiterten Funktion (**Advanced Options**) werden für alle Schnittstellen-Typen im Kapitel 5.3.1.7 ab Seite 131 beschrieben.

5.3.1.4. Virtual LAN

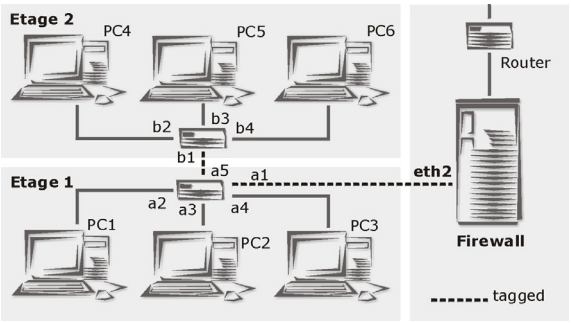


Mit **Virtual LAN** kann ein Netzwerk auf Ethernet-Ebene (Layer 2) in mehrere virtuelle Netzwerksegmente aufgeteilt werden. Dies kann z. B. aus Sicherheitsgründen von Vorteil sein, wenn bestimmte Rechner (Clients) in einem Netzwerk nicht miteinander kommunizieren dürfen. In größeren Netzwerken kann es wiederum praktisch sein, wenn weiter entfernte Rechner (Clients) im selben Netzwerksegment liegen können (Siehe Beispielkonfiguration auf der nächsten Seite).

Auf einem VLAN-fähigen Switch können die Ports in verschiedene Gruppen getrennt werden. Bei einem Switch mit 20 Ports kann z. B. das VLAN Gruppe 1 die Ports 1 bis 10 und das VLAN Gruppe 2 die Ports 11 bis 20 erhalten. Der Rechner an Port 1 kann nun nicht mehr mit dem Rechner an Port 11 kommunizieren. Der Switch wurde demnach in zwei kleinere Switches aufgeteilt.

Für die Verbindung zwischen dem Internet-Sicherheitssystem und den Virtual LANs benötigen Sie eine Netzwerkkarte mit **tag**-fähigem Treiber. Ein **Tag** ist ein kleiner 4-Byte-Header, der an den Ethernet-Header angefügt wird. Dieser angehängte Header enthält die VLAN-Nummer, mit 12 Bit. Es sind also 4095 verschiedene virtuelle LANs möglich. Diese VLAN-Nummer wird im Konfigurationstool als **VLAN Tag** bezeichnet.
Die tagged Pakete dienen nur zur Kommunikation zwischen den VLAN-fähigen Switches und dem Internet-Sicherheitssystem. Die an den Switches angeschlossenen Rechner müssen keine tag-fähigen Netzwerkkarten haben. Allerdings muss der entsprechende Port dieses Switchs als **untagged Port** definiert werden. Die VLAN-fähigen Switches haben meist eine serielle Schnittstelle. Über diese Schnittstelle können mittels Terminalprogramm die verschiedenen Einstellungen durchgeführt werden.

Beispielkonfiguration:



Sie haben mehrere Arbeitsplätze wie in der linken Grafik dargestellt auf zwei Etagen verteilt. Die Computer jeder Etage sind jeweils an einen Switch angeschlossen.
PC1 und PC2 von Etage 1 sollen nun mit PC4 von Etage 2 zum Netzwerksegment VLAN 10 zusammengefasst werden. PC3, PC5 und PC6 werden zu VLAN 20 zusammengefasst.

Auf beiden Switches müssen die Ports konfiguriert werden:

Switch a

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC1)	10	U
3 (PC2)	10	U
4 (PC3)	20	U
5	10,20	T

Switch b

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC4)	10	U
3 (PC5)	20	U
4 (PC6)	20	U

Für PC3 sieht es nun so aus, als währe er nur über einen Switch mit PC5 und PC6 verbunden.

Damit die Rechner nun eine Verbindung zum externen Netzwerk (Internet) erhalten, muss noch die Schnittstelle zum Internet-Sicherheitssystem (im Beispiel eth2) eingestellt werden.

Wichtiger Hinweis:

zur Konfiguration einer Schnittstelle zum **Virtual LAN** benötigen Sie eine Netzwerkkarte mit **tag**-fähigem Treiber. Die vom Internet-Sicherheitssystem unterstützte Hardware ist unter der Internetadresse **http://docs.astaro.org** im Verzeichnis **Hardware Compatibility List for Astaro Security Linux** aufgelistet.

Virtual LAN einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** eine Netzwerkkarte aus.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **VLAN ethernet interface** aus.
6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ **VLAN ethernet interface** durch.

   Address: Weisen Sie der virtuellen Schnittstelle eine IP-Adresse zu. Falls Sie eine statische IP-Adresse eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Netmask: Falls Sie eine statische Netzwerkmaske eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Netzwerkmaske ein. Wenn Sie die Netzwerkmaske durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Default Gateway: Bei einem statischen Default Gateway wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

   VLAN Tag: Tragen Sie in das Eingabefeld den Tag für das virtuelle Netzwerk ein.
7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

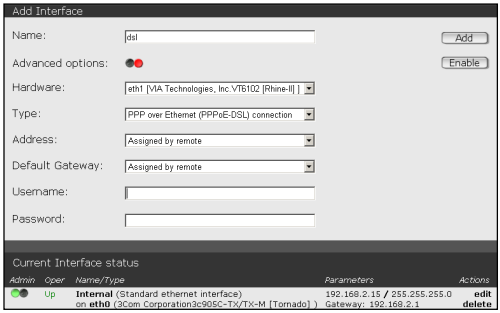
Die neue virtuelle Schnittstelle wird auch in der Tabelle **Hardware Device Overview** angezeigt, da dieser ebenso wie einer Standard-Ethernet-Netzwerkarte eine zusätzliche IP-Adresse zugeordnet werden kann (IP-Aliase). Die **Sys ID** dieser virtuellen Schnittstelle setzt sich aus der Sys ID der verwendeten Netzwerkkarte und des zugeteilten Tag zusammen.

Advanced Options

Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für die erweiterten Funktionen geöffnet.

Die erweiterten Funktion (**Advanced Options**) werden für alle Schnittstellen-Typen im Kapitel 5.3.1.7 ab Seite 131 beschrieben.

5.3.1.5. PPPoE-DSL-Verbindung



Diesen Schnittstellen-Typ benötigen Sie, wenn Sie eine **DSL**-Verbindung zum Internet mit dem Protokoll **PPP over Ethernet** aufbauen möchten. Für die Konfiguration benötigen Sie die DSL-Zugangsdaten inklusive Passwort. Die Daten erhalten Sie von Ihrem Internet Service Provider.

Hinweis:

Die Installation und die nötigen Einstellungen am Internet-Sicherheitssystem speziell für den Internet-Zugang mit **T-DSL** (Telekom Deutschland) wird im Leitfaden **Netzwerk mit T-DSL** erklärt. Nachdem die Schnittstelle geladen wurde, ist das System 24 Stunden am Tag in das externe Netzwerk (Internet) eingewählt. Stellen Sie daher sicher, dass die Abrechnung bei ihrem Provider nach dem Tarif **dsl flat** erfolgt.
Sie finden den aktuellen Leitfaden unter der Internetadresse **http://docs.astaro.org**.

PPP over Ethernet (PPPoE-DSL) einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

   Tipp:

   Wählen Sie als Schnittstelle zum externen Netzwerk (Internet) die Netzwerkkarte mit der Sys ID **eth1** aus.

   Eine Netzwerkkarte auf der bereits die primäre Netzwerkkarten-Adresse eingerichtet wurde, kann hier nicht mehr ausgewählt werden.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **PPP over Ethernet (PPPoE-DSL) connection** aus.

   Für diese Einstellungen benötigen Sie die Zugangsdaten für die DSL-Verbindung.

   Address: Behalten Sie die Default-Einstellung **Assigned by remote** bei, wenn Sie keine feste IP-Adresse haben.
   Bei einer festen IP-Adresse wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein.

Default Gateway: Behalten Sie die Default-Einstellung **Assigned by remote** bei. Mögliche weitere Einstellungen sind **Static** und **None**.

Username: Tragen Sie hier die Zugangsdaten Ihres Providers ein.

Password: Tragen sie hier das Passwort Ihres Providers ein.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

7. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

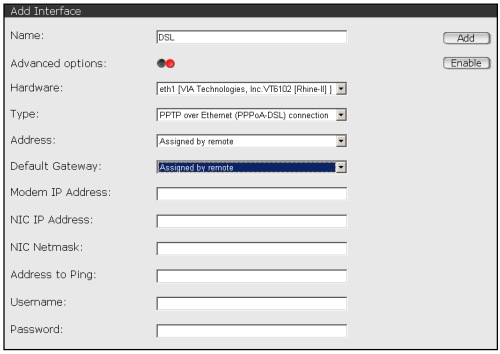
Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Advanced Options

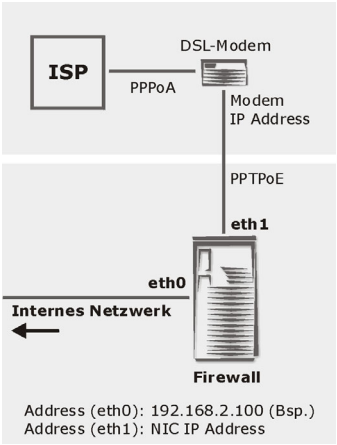
Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für die erweiterten Funktionen geöffnet.

Die erweiterten Funktion (**Advanced Options**) werden für alle Schnittstellen-Typen im Kapitel 5.3.1.7 ab Seite 131 beschrieben.

5.3.1.6. PPTPoE/PPPoA-DSL-Verbindung



Diesen Schnittstellen-Typ benötigen Sie, falls Sie eine **DSL**-Verbindung zum Internet mit dem Protokoll **PPP over ATM** aufbauen möchten. Zur konfiguration benötigen Sie auf dem Internet-Sicherheitssystem eine Ethernet-Netzwerkkarte und ein externes ADSL-Modem mit Ethernet-Anschluss. Die Verbindung zum Internet erfolgt über zwei Teilstrecken. Zwischen dem Internet-Sicherheitssystem und dem ADSL-Modem erfolgt die Verbindung mit dem Protokoll **PPTP over Ethernet**. Die Verbindung vom ADSL-Modem zum Internet Service Provider (ISP) erfolgt mit dem ADSL-Einwahlprotokoll **PPP over ATM** (siehe Grafik).



Für die Konfiguration benötigen Sie die DSL-Zugangsdaten inklusive Passwort. Die Daten erhalten Sie von Ihrem Provider.

Hinweis:

Die Installation und die nötigen Einstellungen am Internet-Sicherheitssystem speziell für den DSL-Zugang mit **AonSpeed** (Telekom Austria) wird im Leitfaden **Netzwerk mit AonSpeed** erklärt. Nachdem die Schnittstelle geladen wurde, ist das System 24 Stunden am Tag in das externe Netzwerk (Internet) eingewählt. Stellen Sie daher sicher, dass die Abrechnung bei ihrem Provider nach einem zeitunabhängigen Tarif erfolgt.
Sie finden den aktuellen Leitfaden unter der Internetadresse **http://docs.astaro.org**.

PPTP over Ethernet (PPPoA-DSL) einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

   Tipp:

   Wählen Sie als Schnittstelle zum externen Netzwerk (Internet) die Netzwerkkarte mit der Sys ID **eth1** aus.

   Eine Netzwerkkarte auf der bereits die primäre Netzwerkkarten-Adresse eingerichtet wurde, kann hier nicht mehr ausgewählt werden.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **PPTP over Ethernet (PPPoA-DSL) connection** aus.

   Für diese Einstellungen benötigen Sie die Zugangsdaten für die DSL-Verbindung.

   Address: Behalten Sie die Default-Einstellung **Assigned by remote** bei, wenn Sie keine feste IP-Adresse haben.
   Bei einer festen IP-Adresse wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein.

   Default Gateway: Behalten Sie die Default-Einstellung **Assigned by remote** bei. Mögliche weitere Einstellungen sind **Static** und **None**.

   Modem IP Address: Tragen Sie hier die IP-Adresse des ADSL-Modems ein. Diese Adresse wird in der Regel vom Provider oder von der Hardware mitgeliefert und kann nicht geändert werden.
   Beispiel: 10.0.0.138 (bei **AonSpeed**)

   NIC IP Address: Tragen Sie hier die IP-Adresse für die Netzwerkkarte auf dem Internet-Sicherheitssystem ein. Die Adresse muss im selben Sub-Netzwerk liegen wie die IP-Adresse des Modems.
   Beispiel: 10.0.0.140 (bei **AonSpeed**)

NIC Netmask: Tragen Sie hier die Netzwerkmaske ein. Beispiel: 255.255.255.0 (bei **AonSpeed**)

Address to Ping: Geben Sie hier die IP-Adresse eines Hosts im Internet ein, der auf ICMP-Ping-Anfragen antwortet (z. B. der DNS-Server Ihres Internet Service Providers). Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird der Verbindungsaufbau abgebrochen.

Username: Tragen Sie hier die Zugangsdaten Ihres Providers ein.

Password: Tragen sie hier das Passwort Ihres Providers ein.

6. Öffnen Sie durch einen Klick auf die Schaltfläche **Enable** das Fenster **Advanced options** für die erweiterten Funktionen an der Schnittstelle.

   Im Eingabefeld **MTU Size** muss ein Wert für die maximale Übertragungsrate in Bytes definiert werden. Per Default ist für die PPTPoE/PPPoA-DSL-Verbindung bereits der Wert **1460** (Bytes) definiert.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden. Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint.

Advanced Options

Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für die erweiterten Funktionen geöffnet.

Die erweiterten Funktion (**Advanced Options**) werden für alle Schnittstellen-Typen im nachfolgenden Kapitel 5.3.1.7 ab Seite 131 beschrieben.

5.3.1.7. Advanced Options

Je nach Schnittstellen-Typ sind bestimmte erweiterte Funktionen vorhanden. Durch einen Klick auf die Schaltfläche **Enable** bei **Advanced options** werden die Eingabefelder und Drop-down-Menüs für diese Funktionen geöffnet.

Proxy ARP: Die Funktion **Proxy ARP** ist nur beim Schnittstellen-Typ **Standard Ethernet Interface** enthalten. Wenn diese Funktion aktiviert ist, wird das Internet-Sicherheitssystem auf der entsprechenden Netzwerkkarte das ARP-Protokoll für alle ihm bekannten Netzwerke setzen. Dies bedeutet, dass das System, stellvertretend für alle anderen direkt angeschlossenen Netzwerke, Pakete aus dem angeschlossenen Netzwerk annehmen und weiterleiten wird.
Diese Funktion wird in einigen Spezialfällen benötigt, um z. B. ein Netzwerk über das Internet-Sicherheitssystem weiterzureichen, falls es nicht möglich ist, korrekte Routen für dieses Netzwerk zu setzen. Dies kann der Fall sein, wenn Sie keinen Zugriff auf den Router Ihres Internet-Providers haben.
Per Default ist **Proxy ARP** ausgeschaltet (**Off**). Sie schalten die Funktion ein, indem Sie im Drop-down-Menü **On** auswählen.

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit dem Modul **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Bandbreitenmanagement kann mit Ausnahme von **Additional address on ethernet interface** auf allen Schnittstellen-Typen durchgeführt werden.
Um die Schnittstelle für das Modul **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Neben der Schnittstellenfreigabe (**QoS Status**) müssen Sie die Werte **Link BW (kbits)** und **Reserved unshaped Bandwidth (kbits)** definieren, wenn Sie das Modul **Quality of Service (QoS)** einsetzen möchten. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.3.7 ab Seite 154 beschrieben.

Link BW (kbits): In dieses Eingabemenü tragen Sie die für diese Schnittstelle verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der vorgeschalteten Schnittstelle oder Router. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Bandbreite z. B. 128 kBit/s, bei einer 2 Megabit Festverbindung
z. B. 2048 kBit/s.

Reserved unshaped Bandwidth (kbits): Wenn Sie die Schnittstelle für das Modul **Quality of Service (QoS)** freigegeben haben (**QoS Status** auf **On**) können Sie hier eine bestimmte Bandbreite in kBit/s für Pakete reservieren, die vom Bandbreitenmanagement nicht berücksichtigt werden soll.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird mit **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.
Bei einer Ethernet-Netzwerkarte beträgt die MTU maximal 1500 Byte.

Bei den folgenden Schnittstellen-Typen ist per Default bereits ein MTU-Wert definiert:

Standard Ethernet Interface: 1500 Byte

PPTP over Ethernet (PPPoA-DSL) connection: 1460 Byte

5.3.2. Routing

Jeder an ein Netzwerk angeschlossene Rechner verwendet eine Routing-Tabelle. Mittels dieser Routing-Tabelle stellt der Rechner fest, ob er ein Datenpaket direkt an den Zielrechner im gleichen Netzwerk oder an einen Router versenden muss.

Static Routes

Für die direkt angeschlossenen Netzwerke trägt das Internet-Sicherheitssystem die entsprechenden Routing-Einträge selbst ein. Weitere Einträge müssen manuell vorgenommen werden. Dies ist z. B. der Fall, wenn im lokalen Netzwerk ein weiterer Router existiert, über den ein bestimmtes Netzwerk erreicht werden soll.
Routen für Netzwerke, die nicht direkt angeschlossen sind, aber über einen Befehl oder eine Konfigurationsdatei in die Routing-Tabelle eingetragen werden, bezeichnet man als statische Routen.

In diesem Menü können Sie festlegen, welches Netzwerk zu welcher Netzwerkkarte oder zu welcher externen IP-Adresse geroutet wird.

Statisches Routing definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Routing**.

2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Static Route** zu öffnen.

3. Wählen Sie im Drop-down-Menü **Network** das Netzwerk aus.
   Im Auswahlmenü **Network** sind alle statischen sowie die in den Menüs **Networks** und **Interfaces** neu definierten Netzwerke enthalten.

4. Wählen Sie im Drop-down-Menü **Target** das Ziel aus.
   Namen in zwei spitzen Klammern kennzeichnen Netzwerk-

karten (**Interfaces**). Bei Namen ohne Klammern handelt es sich um einen Host oder um einen Router.

5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

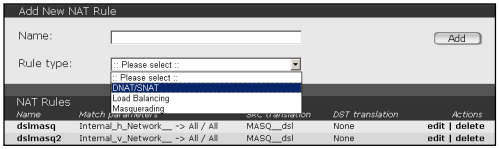
Nach erfolgreicher Definition wird die neue Route in die Tabelle **Static Routes** importiert. Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag wieder gelöscht.

Kernel Routing Table

Im Fenster **Kernel Routing Table** werden alle vom System automatisch generierten sowie die statischen Routen aufgelistet, wobei die Routen nach der Größe der Netzmasken sortiert sind. Die Routen mit der kleinsten Netzmaske stehen an oberster Stelle. Das System arbeitet die Routen in der dargestellten Reihenfolge ab. Die erste zutreffende Route wird verwendet.
Per Default sind die Routen der Netzwerkkarten bereits eingetragen und nicht editierbar.

5.3.3. NAT/Masquerading

5.3.3.1. NAT



Die Funktion **Network Address Translation (NAT)** dient zur Umsetzung der - meist privaten - IP-Adressen eines Netzwerkes auf andere - meist öffentliche - IP-Adressen eines anderen Netzwerkes. NAT ermöglicht damit mehreren PCs in einem LAN, einerseits die IP-Adresse des Internet-Access-Routers für den Internet-Zugang zu nutzen, und andererseits versteckt es das LAN hinter der im Internet registrierten IP-Adresse des Routers.

Wenn ein Client im LAN ein IP-Paket an den Router schickt, wandelt NAT die Adresse des Absenders in eine gültige IP-Adresse um (die ihm etwa der Provider zugeteilt hat), bevor es ins Internet weitergereicht wird. Kommt von der entfernten Station eine Antwort auf dieses Paket zurück, wandelt NAT die Empfängeradresse wieder in die ursprüngliche IP-Adresse der

lokalen Station um und stellt das Paket ordnungsgemäß zu. Theoretisch kann NAT interne Netzwerke (LANs) mit beliebig vielen Clients verwalten.

Durch **Destination Network Address Translation (DNAT)** wird die Zieladresse (**Destination Address**) der IP-Pakete umgeschrieben. Dies ist besonders interessant, wenn Sie ein privates Netzwerk hinter Ihrem Internet-Sicherheitssystem betreiben und Netzwerkdienste im Internet verfügbar machen wollen.

Wichtiger Hinweis:

DNAT kann nicht in Verbindung mit **PPTP Roadwarrior Access** verwendet werden.

Beispiel:

Ihr internes Netzwerk hat den Addressraum 192.168.0.0/ 255.255.255.0. Sie möchten nun Ihren Webserver, der auf dem Server mit der IP-Addresse 192.168.0.20 auf Port 80 läuft, für Clients aus dem Internet erreichbar machen.
Die Clients können dessen Adresse nicht direkt ansprechen, da der Adressbereich 192.168 im Internet nicht geroutet wird. Es ist jedoch möglich, vom Internet aus die externe Addresse Ihres Internet-Sicherheitssystems anzusprechen. Mit **DNAT** können Sie z. B. den Port 80 auf der externen Schnittstelle des Internet-Sicherheitssystems auf den Webserver umleiten.

Hinweis:

Die Einstellungen für einen Webserver hinter dem Internet-Sicherheitssystem werden im Leitfaden **Web Server/DNAT** beschrieben.
Sie finden den aktuellen Leitfaden unter der Internetadresse **http://docs.astaro.org**.

Die Funktionalität von **Source Network Address Translation (SNAT)** entspricht der von **DNAT**, mit dem Unterschied, dass statt der Zieladresse (**Destination Address**) der IP-Pakete die Quelladresse (**Source Address**) umgeschrieben wird.
Dies kann in komplexen Netzwerken nützlich sein, um Antworten

auf Verbindungen in andere Netzwerke oder auf andere Hosts umzuleiten.

Tipp:

Um eine einfache Anbindung von privaten Netzwerken an das externe Netzwerk (Internet) zu erreichen, sollten Sie anstatt **SNAT** die Funktion **Masquerading** verwenden.

Im Gegensatz zum (dynamischen) **Masquerading** handelt es sich bei **SNAT** um eine statische Adressumsetzung, d. h. jeder internen IP-Adresse wird genau eine extern sichtbare **IP-Adresse** zugewiesen.

DNAT/SNAT-Regel definieren:

Hinweis:

Um den Port 443 (HTTPS) umzuleiten, müssen Sie im Menü **System/Settings** den **WebAdmin TCP Port** auf einen anderen Wert ändern (z. B. 1443).
Diese Funktion wird in Kapitel 5.1.1 im Abschnitt **WebAdmin Settings** beschrieben.

Hinweis:

Da die Adressumsetzung vor der Filterung durch **Paketfilterregeln** erfolgt, müssen Sie im Menü **Packet Filter/Rules** die entsprechenden Regeln setzen.
Das Setzen der Paketfilterregeln wird ausführlich in Kapitel 5.4 ab Seite 164 beschrieben.

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT/Masquerading**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **NAT-Regel**.

3. Wählen Sie im Drop-down-Menü **Rule type** die Funktion **DNAT/SNAT** aus.

   Anschließend öffnet sich das Fenster **Add new NAT Rule**.

4. Definieren Sie im Fenster **Packets to match** welche Pakete zu einer neuen Adresse umgeleitet bzw. in einen anderen Dienst übersetzt werden sollen.

   Damit eine gültige DNAT/SNAT-Regel definiert werden kann, muss in diesem Fenster mindestens ein Parameter ausgewählt werden. Die Einstellung **No match** hat zur Folge, dass zwischen den Parametern in dieser Auswahl nicht unterschieden wird.

   Source address: Wählen Sie die original Quelladresse aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

   Destination address: Wählen Sie die original Zieladresse aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

   Service: Wählen Sie den original Dienst aus. Dieser Dienst besteht aus Quell- und Zielport der Pakete oder einem Protokoll, z. B. TCP.

   Hinweis:

   Ein **Dienst** (**Service**) kann nur umgeleitet werden, wenn auch die kommunizierenden Adressen umgeleitet werden. Des Weiteren kann ein Dienst nur in einen Dienst mit gleichem Protokoll übersetzt werden.

5. Definieren Sie mit den folgenden Drop-down-Menüs wohin die Pakete umgeleitet werden sollen.

   Damit eine gültige DNAT/SNAT-Regel definiert werden kann, muss in diesem Fenster mindestens ein Parameter ausgewählt werden. Wenn Sie die original Adresse auf ein gesamtes Netzwerk umleiten, werden die darin enthaltenen IP-Adressen der Reihe nach ausgewählt.

   Change source to (SNAT): Wählen Sie die neue Quelladresse für die IP-Pakete aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

   Service source: Dieses Drop-down-Menü wird angezeigt, wenn Sie bei **Change source to** eine Adresse ausgewählt haben. Es können hier nur Dienste (Services) mit einem Quellport ausgewählt werden.

Change destination to (DNAT): Wählen Sie die neue Zieladresse für die IP-Pakete aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

Service destination: Dieses Drop-down-Menü wird angezeigt, wenn Sie bei **Change destination to** eine Adresse auswählen.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Nach erfolgreicher Definition wird die neue DNAT/SNAT-Regel in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen in der NAT-Tabelle weitere Funktionen zur Verfügung.

Weitere Funktionen

Einträge editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Einträge löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.3.2. Masquerading

Masquerading ist eine Sonderform von **SNAT**, bei der viele private IP-Adressen auf eine einzige öffentliche IP-Adresse umgesetzt werden, d. h. Sie verbergen interne IP-Adressen und Netzwerkinformationen nach außen.

Die Unterschiede zwischen Masquerading und SNAT sind:

- Bei Masquerading geben Sie nur ein Quellnetzwerk an. Es werden automatisch alle Dienste (Ports) in die Übersetzung mit einbezogen.
- Die Übersetzung findet nur dann statt, wenn das Paket über die angegebene Netzwerkkarte versendet wird. Als neue Quelladresse wird stets die Adresse dieser Netzwerkkarte in die Datenpakete eingefügt.

Damit eignet sich **Masquerading** besonders, um private Netzwerke in einem LAN hinter einer offiziellen IP-Adresse an das Internet anzubinden.

Masquerading definieren:

Legen Sie über die Drop-down-Menüs fest, welches Netzwerk auf welcher Netzwerkkarte maskiert werden soll. Im Normalfall wählt man die externe Netzwerkkarte.

Hinweis:

Damit von den Clients aus dem hier definierten Netzwerk eine Verbindung zum Internet aufgebaut werden kann, müssen im Menü **Packet Filter/Rules** die entsprechenden Regeln gesetzt werden.
Das Setzen der Paketfilterregeln wird ausführlich in Kapitel 5.4 ab Seite 164 beschrieben.

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT/Masquerading**.
2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **NAT-Regel**.
3. Wählen Sie im Drop-down-Menü **Rule type** die Funktion **Masquerading** aus.

   Anschließend öffnet sich das Fenster **Add new NAT Rule**.
4. Wählen Sie im Drop-down-Menü **Network** ein Netzwerk aus.
5. Wählen Sie im Drop-down-Menü **Interface** eine Netzwerkkarte aus.
6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Nach erfolgreicher Definition wird die Masquerading-Regel in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen weitere Funktionen zur Verfügung.

Weitere Funktionen

Masquerading editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Masquerading löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.3.3. Load Balancing

Mit **Load Balancing** können Sie auf den Ports ankommende Datenpakete, z. B. SMTP oder HTTP auf verschiedene Server hinter dem Internet-Sicherheitssystem verteilen.

Beispiel: Sie haben in Ihrer DMZ zwei HTTP-Server mit den IP-Adressen 192.168.66.10 und 192.168.66.20. Mit Load Balancing können Sie nun die auf der externen Netzwerkkarte für den Dienst HTTP ankommenden Datenpakete auf die zwei HTTP-Server verteilen.

Bevor Sie die Load Balancing-Regel definieren können, müssen Sie im Menü **Definitions/Networks** die zwei HTTP-Server als Netzwerke, bestehend aus je einem Host, definieren und anschließend im Menü **Definitions/Network Groups** zu einer Netzwerkgruppe zusammenfasen.
Das Hinzufügen von Netzwerken (**Networks**) und die Erstellung von Netzwerkgruppen (**Network Groups**) wird in den Kapiteln 5.2.1 und 5.2.2 beschrieben.

Danach können Sie, wie nachfolgend beschrieben, die Load Balancing-Regel definieren.

Load Balancing definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT/Masquerading**.

   Anschließend öffnet sich das Fenster **Add new NAT Rule**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die Load Balancing-Regel.

3. Wählen Sie im Drop-down-Menü **Rule type** die Funktion **Load Balancing** aus.

4. Wählen Sie im Fenster **Pre-Balancing Target** die original Zieladresse und den entsprechenden Dienst (**Service**) aus.

   Address: Tragen Sie hier die original Ziel-Adresse ein. In der Regel ist dies die externe Adresse des Internet-Sicherheitssystems.

   Service: Wählen Sie hier den original Zielport (Dienst) aus.

5. Wählen Sie im Drop-down-Menü **Post-Balancing Target Group** die neue Adresse aus. In der Regel ist dies eine Netzwerkgruppe aus einzelnen Hosts.

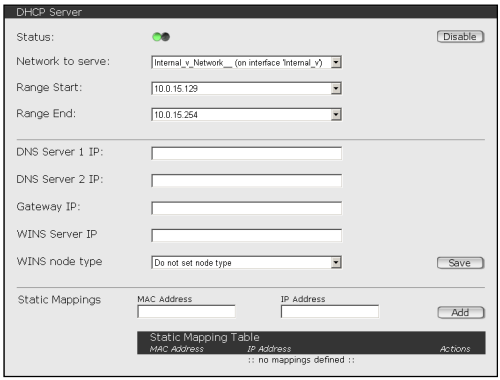
Nach erfolgreicher Definition wird die Load Balancing-Regel in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen weitere Funktionen zur Verfügung.

Weitere Funktionen

Load Balancing editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Load Balancing löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.4. DHCP Server



Das **Dynamic Host Configuration Protocol (DHCP)** weist den angeschlossenen Rechnern (Clients) aus einem festgelegten Bereich von IP-Adressen automatisch Adressen zu und spart so bei größeren Netzwerken viel Konfigurationsarbeit. Des Weiteren kann den Clients die Adresse des Default Gateways (Routers) und der zuständigen Nameserver (DNS) zugewiesen werden.

Neben der einfacheren Konfiguration der Clients und der Möglichkeit, mobile Rechner problemlos in unterschiedlichen Netzwerken zu betreiben, lassen sich in einem DHCP-Netzwerk Fehler einfacher lokalisieren, da die Konfiguration des Netzwerks, geht es um die Adressen, primär von der Konfiguration des DHCP-Servers abhängt. Außerdem lassen sich Adressbereiche effektiver nutzen, da keineswegs alle Hosts gleichzeitig im Netzwerk aktiv sind. Die IP-Adressen können so je nach Bedarf nacheinander an verschiedene Hosts vergeben werden.

DHCP-Server konfigurieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Server**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich das Fenster **DHCP Server**.

3. Wählen Sie im Drop-down-Menü **Network to serve** das Netzwerk aus, in dem die IP-Adressen zugewiesen werden sollen.

4. Bestimmen Sie mit den Drop-down-Menüs **Range Start** und **Range End** den IP-Adressenbereich.

Die Einstellungen werden anschließend ohne weitere Bestätigung übernommen.

DNS-Server und Gateway IP-Adressen zuweisen:

Sie können den Clients weitere Parameter zur Netzwerkkonfiguration übergeben. Dazu gehören die DNS-Server-Adressen und das Default Gateway, welches die Clients verwenden sollen. In der Regel wird das Internet-Sicherheitssystem selbst diese Aufgaben übernehmen. In diesem Fall sollten Sie die interne Adresse ihres Internet-Sicherheitssystems in diesen Einstellungen angeben.

Die Konfiguration des DNS-Proxy erfolgt im Menü **Proxies/DNS**. Die Funktionalität des DNS-Proxy wird in Kapitel 5.5.2 ab Seite 183 beschrieben.

Für NetBIOS-Netzwerke kann zur Namensauflösung ein **WINS**-Server eingetragen werden. WINS ist die Abkürzung für Windows Internet Name Service. Ein WINS-Server ist ein MS Windows NT-Server, auf dem Microsoft TCP/IP und die WINS-Serversoftware ausgeführt werden. Auf WINS-Servern wird eine Datenbank verwaltet, in der Computernamen den IP-Adressen so zugeordnet werden, dass die Benutzer problemlos mit anderen Computern unter Benutzung der WINDOWS-Techniken kommunizieren können und dabei alle Vorteile von TCP/IP nutzen können.

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Server**.

   Falls der DHCP-Server bereits eingeschaltet ist, öffnet sich das Fenster **DHCP Server**.

2. Tragen Sie in die Eingabefelder **DNS Server 1** und **DNS Server 2** die IP-Adressen der Nameserver ein.

3. Tragen Sie in das Eingabefeld **Gateway IP** die IP-Adresse des Default Gateways ein.

4. Falls Sie einen **WINS**-Server zuweisen möchten, führen Sie die folgenden zwei Einstellungen durch:

   WINS Server IP: Tragen Sie hier die IP-Adresse des WINS-Servers ein.

   WINS node type: Wählen Sie im Drop-down-Menü die Methode aus, die der Client zur Namensauflösung anwenden soll. Falls die Einstellung **Do not set note type** ausgewählt ist, wird das Vorgehen vom Client selbst bestimmt.

5. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Statische Adresszuweisung konfigurieren:

Hier können Sie einigen oder sogar allen Clients in diesem Netzwerk eine bestimmte IP-Adresse statisch zuweisen. Dafür benötigen Sie die MAC-Adresse der Netzwerkkarte dieses Clients.

Wie Sie die MAC-Adresse der Netzwerkkarte erhalten wird ab Seite 115 erklärt.

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Server**.

2. Tragen Sie in das Eingabefeld **MAC Address** die MAC-Adresse der Netzwerkkarte ein. Die MAC-Adresse muss wie im Beispiel dargestellt eingegeben werden.
   Beispiel: 00:04:76:16:EA:62

3. Tragen Sie in das Eingabefeld **IP Address** die IP-Adresse ein. Diese IP-Adresse muss in dem Bereich enthalten sein, den Sie zuvor mit den Auswahlmenüs **Range Start** und **Range End** definiert haben.

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Anschließend wird die statische IP-Adresszuweisung in die Tabelle **Static Mapping Table** importiert. Durch einen Klick auf die Schaltfläche **delete** kann der Eintrag wieder gelöscht werden.

DHCP Server Leases

In der Tabelle **DHCP Server Leases** werden die aktuellen IP-Adresszuweisungen dargestellt. Für ein und dieselbe IP-Adresse können mehrere Zuweisungen enthalten sein, allerdings ist immer nur der letzte Eintrag gültig. Diese Tabelle wird nur angezeigt, wenn Einträge vorhanden sind.

5.3.5. Portscan Detection

Mit **Portscan Detection** oder auch **PSD** sind Sie in der Lage, mögliche Angriffe durch Unbefugte zu erkennen. Sogenannte Portscans werden meist von Hackern durchgeführt, um ein abgesichertes Netzwerk nach erreichbaren Diensten **(Services)** zu durchsuchen. Um in ein System einzudringen bzw. eine **Denial-of-Service (DoS)**-Attacke zu starten, benötigt der Angreifer Informationen zu den Netzwerk-Diensten. Wenn solche Informationen vorliegen, ist der Angreifer möglicherweise in der Lage, gezielt die Sicherheitslücken dieser Dienste auszunutzen. Netzwerkdienste, die die Internet-Protokolle TCP und UDP verwenden, sind über bestimmte Ports erreichbar und diese Port-Zuordnung ist im Allgemeinen bekannt, z. B. ist der Dienst SMTP in der Regel dem TCP Port 25 zugeordnet. Die von Diensten verwendeten Ports werden als „offen" (open) bezeichnet, da es möglich ist, eine Verbindung zu ihnen aufzubauen. Die unbenutzten Ports werden hingegen als „geschlossen" (closed) bezeichnet – Versuche zu ihnen eine Verbindung aufzubauen scheitern. Damit nun der Angreifer herausfinden kann, welche Ports „offen" sind, verwendet er ein spezielles Software-Tool, den Port Scanner. Dieses Programm versucht mit mehreren Ports auf dem Zielrechner eine Verbindung aufzubauen. Falls dies gelingt, meldet es die entsprechenden Ports als „offen" und der Angreifer hat die nötigen Informationen, welche Netzwerkdienste auf dem Zielrechner verfügbar sind.

Der Port Scanner kann z. B. folgende Informationen liefern:

```
Interesting ports on (10.250.0.114):
          (The 1538 ports scanned but not shown below
          are in state: closed)
          Port       State    Service
          25/tcp     open     smtp
          135/tcp    open     loc-srv
          139/tcp    filtered netbios-ssn
          445/tcp    open     Microsoft-ds
          1032/tcp   open     iad3
```

Da den Internetprotokollen TCP und UDP je 65535 Ports zur Verfügung stehen, werden die Ports in sehr kurzen Zeitabständen gescannt. Wenn nun von derselben IP-Adresse mehrere Versuche registriert werden, mit immer anderen Ports Ihres Systems Verbindung aufzunehmen bzw. Informationen an diese zu senden, dann handelt es sich mit ziemlicher Sicherheit um einen Portscan.
PSD entdeckt diese Portscans und informiert per E-Mail den Administrator sobald der Vorgang protokolliert wurde. Anschließend können Sie entscheiden, welche Maßnahme gegen weitere Verbindungen vom Port Scanner des Angreifers durchgeführt werden soll.

Sicherheitshinweis:

Achten Sie als Administrator darauf, dass auf dem System immer die aktuellsten Sicherheits-Patches eingespielt sind.
Der Up2Date-Service wird ausführlich in Kapitel 5.1.3 ab Seite 52 beschrieben.

Portscan Detection einschalten/ausschalten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Portscan Detection**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich das Fenster **Portscan Detection**.

3. Wählen Sie im Drop-down-Menü **Action taken on portscanner traffic** die Maßnahme gegen den erkannten Portscanner aus.

   Accept (no interception): Es wird keine Maßnahme gegen den Portscanner ergriffen – es erfolgt nur eine Meldung.

   Obwohl diese Einstellung keine Maßnahmen gegen den Portscanner einleitet, ist dies die Standardeinstellung. Unter Umständen kann es vorkommen, dass auch normale Netzwerkaktivitäten als ein Portscan interpretiert werden. Die restriktiven Maßnahmen können in diesem Fall die Arbeit behindern.

Drop (blackhole): Die nachfolgenden Pakete einer Portscansequenz werden verworfen und es kommt keine Verbindung zu Stande. Für den Portscanner ist dieser Port „gefiltert" (filtered).

Reject (reply with icmp deny): Die Verbindungsanfragen des Angreifers werden mit einem RST ACK „port unreachable" zurückgewiesen. Dadurch wird der Port als „geschlossen" (closed) ausgegeben und dem Angreifer bleiben die Dienste (Services) versperrt.

Falls Sie **Drop** oder **Reject** ausgewählt haben, bleibt die gewählte Aktion solange in Kraft, bis der portscan-typische Datenverkehr aufhört.

4. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

PSD Network Exclusion

Normale Netzwerkaktivitäten, z. B. **Traceroute** oder ein **FTP**-Datenverkehr mit vielen kleinen Dateien können durch **PSD** als ein Portscan interpretiert werden. Aus diesem Grund ist es sinnvoll, bestimmte Quell- und Zielnetzwerkkombinationen vom **PSD** auszuschließen.

Netzwerk vom PSD ausschließen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Portscan Detection**.

2. Führen Sie im Fenster **PSD Network Exclusion** folgende Einstellungen durch.

   Source network: Wählen Sie das Quellnetzwerk aus.

   Destination network: Wählen Sie das Zielnetzwerk aus.

3. Übernehmen Sie die Einstellungen durch einen Klick auf die Schaltfläche **Add**.

In vom **PSD** ausgenommenen Netzwerkkombinationen werden keine Portscans mehr erkannt.

5.3.6. PPTP Roadwarrior Access

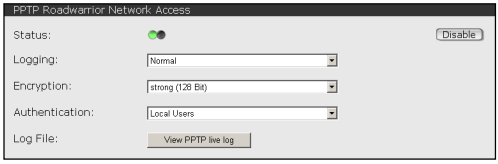
Mit **Point-to-Point Tunneling Protocol (PPTP)** können Sie einzelnen Hosts den Zugang zu Ihrem Netzwerk über einen verschlüsselten Tunnel ermöglichen. **PPTP** ist wesentlich einfacher einzurichten und benötigt auf Microsoft Windows Clients keine zusätzliche Software.

PPTP ist in Microsoft Windows ab Version 95 enthalten. Um **PPTP** mit dem Internet-Sicherheitssystem verwenden zu können, muss der Client die MSCHAPv2-Authentifizierung unterstützen. Zu diesem Zweck muss auf MS Windows 95 und 98 Clients ein Update aufgespielt werden. Dieses Update finden Sie bei Microsoft unter:

http://support.microsoft.com/support/kb/articles/Q191/5/40.ASP

Sie benötigen dort das VPN-Update und eventuell das RAS-Update, wenn Sie Microsoft Windows 95 verwenden.

PPTP Roadwarrior Network Access



In diesem Fenster schalten Sie den **PPTP Roadwarrior**-Zugang durch einen Klick auf die jeweilige Schaltfläche **Enable**/**Disable** ein- und aus.

Logging: Hier stellen Sie ein, wie ausführlich die Informationen in den **PPTP Roadwarrior Access Logs** protokolliert werden. Stellen Sie den Protokollumfang auf **Ausführlich** (**Extensive**), wenn Verbindungsprobleme zum Host auftreten und öffnen anschließend das **Live Log**-Fenster. Sobald Sie nun die Verbindung starten, können Sie den Vorgang in Echtzeit nachverfolgen.

Encryption: Hier stellen Sie die Verschlüsselungsstärke (40 Bit oder 128 Bit) dieser VPN-Verbindungsart ein. Beachten Sie, dass bei Microsoft Windows 2000 im Gegensatz zu Windows 98 und Windows ME nur die Verschlüsselungsstärke 40 Bit installiert ist. Sie benötigen zusätzlich das **High Encryption Pack** oder **Service Pack 2**. **SP2** kann allerdings später nicht mehr deinstalliert werden.

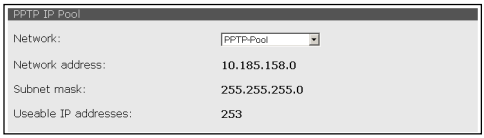
Sicherheitshinweis:

Stellen Sie im Drop-down-Menü **Encryption** die Verschlüsselungsstärke immer auf **Strong** (128 Bit) ein, es sei denn der Endpunkt (Host) unterstützt diese Verschlüsselungsstärke nicht.

Mit dem Drop-down-Menü **Authentication** wählen Sie die Authentifizierungsmethode aus. Wenn Sie im Menü **System/User Authentication** einen RADIUS-Server konfiguriert haben, können Sie hier auch RADIUS-Authentifizierung einsetzen.
Die Konfiguration des Microsoft IAS RADIUS-Servers und die Einstellungen im WebAdmin werden in Kapitel 5.1.6 ab Seite 66 erklärt.

Im Fenster **PPTP Live Log** werden wichtige Vorgänge oder Fehlermeldungen dargestellt. Den Umfang der Meldungen können Sie mit dem Auswahlmenü **Logging** bestimmen.

PPTP IP Pool



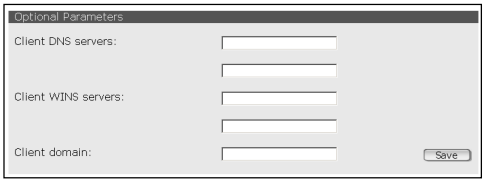
Hier legen Sie fest, welche IP-Adressen den Hosts bei der Einwahl zugewiesen werden. Per Default-Einstellung wird beim ersten Aktivieren der PPTP-Funktion ein Netzwerk aus dem privaten IP-Bereich 10.x.x.x ausgewählt. Dieses Netzwerk wird **PPTP Pool** genannt und kann für alle anderen Funktionen des Internet-Sicherheitssystems genutzt werden, in denen Netzwerkdefinitionen verwendet werden. Falls Sie ein anderes Netzwerk verwenden wollen, können Sie entweder die bestehende PPTP Pool-Definition verändern, oder ein anderes definiertes Netzwerk als PPTP Pool festlegen.

Die PPTP-Benutzer legen Sie in **Definitions/Users** an. Dort ist es möglich, bestimmten Benutzern eigene IP-Adressen zuzuweisen. Diese IP-Adressen müssen nicht Bestandteil des verwendeten Pools sein. Sollen diese Adressen im Paketfilter oder an anderer Stelle der Konfiguration verwendet werden, müssen sie entweder als einzelne Hosts (Netzmaske 255.255.255.255) oder als Teil eines übergeordneten Netzwerkes definiert werden.

Hinweis:

Falls Sie für Ihren **PPTP Pool** private IP-Adressen, wie z. .B. das vordefinierte Netzwerk verwenden, müssen Sie **Masquerading** oder **NAT**-Regeln für den PPTP Pool erstellen, wenn ein Zugriff auf das Internet von den PPTP-Hosts aus erwünscht ist.

Optional Parameters



In diesem Fenster können Sie den Hosts während des Verbindungsaufbaus zusätzlich bestimmte Name-(DNS)- und Windows-Server zuweisen.

Verbindung mit MS Windows 2000:

Hier wird in einem Beispiel-Szenario beschrieben, wie eine Verbindung mit PPTP Roadwarrior Access konfiguriert wird, wenn auf dem Host Microsoft Windows 2000 installiert ist.

1. Öffnen Sie im Verzeichnis **Network** das Menü **PPTP Roadwarrior Access**.

2. Schalten Sie im Fenster **PPTP Roadwarrior Network Access** den PPTP-Status durch einen Klick auf die Schaltfläche **Enable** ein (Statusampel zeigt Grün).

3. Bestimmen Sie im Drop-down-Menü **Encryption** die Verschlüsselungsstärke. Sie können zwischen **weak (40 Bit)** und **strong (128 Bit)** wählen.

   Beachten Sie, dass bei Microsoft Windows 2000 im Gegensatz zu MS Windows 98 und Windows ME nur die Verschlüsselungsstärke 40 Bit standardmäßig installiert ist.
   Für eine 128 Bit-Verschlüsselungsstärke benötigen Sie zusätzlich das **High Encryption Pack** oder **Service Pack 2**. **SP2** kann aber später nicht mehr deinstalliert werden.

   Die ausgewählte Verschlüsselungsstärke wird sofort übernommen.

Wichtiger Hinweis:

Damit die Verbindung zustande kommt, muss auf beiden Seiten die gleiche Verschlüsselungsstärke eingestellt sein. Wenn im **WebAdmin** die Verschlüsselungsstärke 40 Bit eingestellt ist und Sie auf der Gegenstelle in MS Windows 2000 die Verschlüsselungsstärke 128 Bit auswählen, kommt fälschlicherweise die Meldung unter Windows, dass die Verbindung besteht.

4. Legen Sie nun fest, welche IP-Adressen den Hosts bei der Einwahl zugewiesen werden sollen. Wählen Sie im Fenster **PPTP IP Pool** mit dem Drop-down-Menü **Network** ein Netzwerk aus. Per Default-Einstellung ist hier bereits **PPTP Pool** ausgewählt.
   Das ausgewählte Netzwerk wird sofort übernommen.

   Anschließend wird unter dem Auswahlmenü die IP-Adresse des Netzwerks, die Netzwerkmaske und die Anzahl der freien IP-Adressen angezeigt.
   Dem Benutzer wird später automatisch eine IP-Adresse zugeordnet.

5. Im Fenster **Optional Parameters** können Sie den Hosts während der Verbindung bestimmte DNS- und Windows-Server zuweisen. Es können jeweils zwei Server eingetragen werden.

   Client DNS servers: Tragen Sie hier die IP-Adressen der DNS-Server ein.

   Client WINS servers: Tragen Sie hier die IP-Adressen der Windows-Server ein.

   Client domain: Tragen Sie hier die Domain ein, die der Client bei DNS-Anfragen an Hostnamen anhängen soll.

   Speichern Sie die Eingaben anschließend durch einen Klick auf die Schaltfläche **Save**.

Die weitere Konfiguration erfolgt am Host des Benutzers. Der Benutzer benötigt zur weiteren Konfiguration die IP-Adresse des Servers sowie einen Benutzernamen und Passwort. Diese Angaben werden vom Administrator des Internet-Sicherheitssystems vergeben.

1. Klicken Sie in Microsoft Windows 2000 auf **Start/Einstellungen/Netzwerk und DFÜ-Verbindungen**.

2. Klicken Sie auf das Icon **Neue Verbindung erstellen**.

   Der **Netzwerksverbindungs-Assistent** öffnen sich.

   Klicken Sie auf die Schaltfläche **Weiter**.

3. Wählen Sie die folgende Option aus: **Verbindung mit einem privaten Netzwerk über das Internet herstellen.** Klicken Sie anschließend auf die Schaltfläche **Weiter**.

4. Falls Sie eine permanente Verbindung ins Internet haben, wählen Sie die folgende Option aus: **Keine Anfangsverbindung automatisch wählen**.
   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

   Falls Sie sich zuerst über einen Provider in das Internet einwählen, klicken Sie auf die Option **Andere Verbindung zuerst wählen** und wählen im Auswahlmenü Ihren Provider aus. Diese Einstellungen können Sie auch später im Dialog **Eigenschaften** vornehmen bzw. ändern.

5. Tragen Sie nun in das Eingabefeld **Zieladresse** die IP-Adresse des Servers ein.
   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

6. Bestimmen Sie nun im Fenster **Verfügbarkeit der Verbindung** ob der PPTP-Zugang für alle Benutzer oder nur für Sie selbst zu Verfügung stehen soll.
   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

7. Geben Sie im Fenster **Fertigstellen des Assistenten** in das Eingabefeld einen beliebigen Namen für die PPTP-Verbindung ein.
   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

8. Mit einem Klick mit der rechten Maustaste auf das neue Symbol im Menü **Start/Einstellungen/Netzwerk und DFÜ-Verbindungen** können Sie im Dialog **Eigenschaften** in verschiedenen Registerkarten weitere Einstellungen vornehmen oder ändern:

   Allgemein: Hier können Sie den Hostnamen oder die Ziel-IP-Adresse ändern. Falls vor der PPTP-Verbindung eine Verbindung zum Internet Service Provider (ISP) aufgebaut

werden muss, stellen Sie diese im Fenster **Erste Verbindung** ein.

Optionen: Hier können Sie die Wähl- und Wahlwiederholungsoptionen definieren.

Sicherheit: Wählen Sie die Option **Erweitert (Benutzerdefinierte Einstellungen)**. Klicken Sie anschließend auf die Schaltfläche **Einstellungen**. Belassen Sie die Standardeinstellungen in diesem Menü.

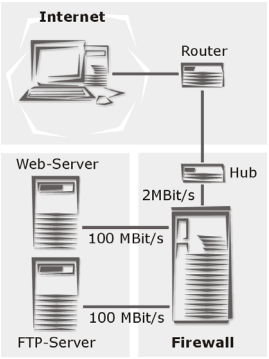
Netzwerk: Wählen Sie im Auswahlmenü **Typ des anzurufenden VPN-Servers** die Option **Point-to-Point-Tunneling-Protokoll (PPTP)** aus.

Gemeinsame Nutzung: Hier können Sie die Nutzungsbedingungen für die PPTP-Verbindung definieren.

Anschließend wird die PPTP-Verbindung mit einem Klick auf das neue Icon im Menü **Start/Einstellungen/Netzwerk und DFÜ-Verbindungen** gestartet.

Weitere Informationen erhalten Sie in der Regel vom Administrator des Netzwerks.

5.3.7. Quality of Service (QoS)



Die Übertragungsleistung eines Leitungssystems wird als Bandbreite bezeichnet und wird hier in kBit/s angegeben. Falls die anfallende Datenmenge die Leistungsgrenze überschreitet, kann die Kommunikation entweder sehr langsam werden oder sogar gänzlich zusammenbrechen.

In der linken Grafik ist z. B. ein Netzwerk mit einem Web-Server und einem FTP-Server dargestellt. Beide Server teilen sich eine 2MBit-Leitung zum Internet. Protokollbedingt nutzen TCP-basierende Aplikationen, z. B. FTP, immer die volle Bandbreite. Dies kann zur Folge haben, dass für den Web-Server nicht mehr genug Bandbreite zur Verfügung steht.

Mit dem Modul **Quality of Service (QoS)** können Sie den Datenpaketen durch Setzen von Regeln einen definierten Anteil der vorhandenen Bandbreite zuweisen. Falls für ein Datenpaket keine Regeln definiert wurden, wird die **Best-Effort**-Methode angewendet, d. h. dass das Paket erst versendet wird, wenn genug Bandbreite zur Verfügung steht. Dies hat im **Worst Case** zur Folge, dass bei einem Datenstau das Datenpaket zuerst blockiert wird.
Damit die Datenpakete vom Web-Server, wie in dem Beispiel dargestellt, ausreichend Bandbreite zur Verfügung gestellt bekommt, kann man nun folgende zwei Regeln setzen:

1. Regel für Datenpakete vom FTP-Server:

From (Client): FTP-Server
Service: FTP
To (Server): Internet
Weight: medium (2)
Borrow: borrow

2. Regel für Datenpakete vom Web-Server:

From (Client): Web-Server
Service: HTTP
To (Server): Internet
Weight: medium (2)
Borrow: borrow

Mit diesen Regeln wird im **Worst Case** jedem Datenpaket von diesen beiden Servern je die Hälfte der Bandbreite (1MBit/s) zugewiesen. Falls Sie z. B. dem FTP-Server im Drop-down-Menü **Weight** den Anteil **high (3)** und dem Web-Server den Anteil **low (1)** zuweisen, erhält das Datenpaket vom FTP-Server 1,5 Mbit/s und das Datenpaket vom Web-Server 0,5Mbit/s der Bandbreite.

QoS-Regel setzen:

Bevor Sie in diesem Menü die Regeln für das Bandbreitenmanagement setzen können, müssen Sie im Menü **Network/ Interfaces** die entsprechende Schnittstelle für das Modul **QoS** freigeben und die Werte **Link BW** und **Reserved unshaped BW** definieren.
Die speziellen Einstellungen auf der Schnittstelle für das Modul **QoS** werden im Kapitel 5.3.1.7 ab Seite 131 erklärt.

1. Öffnen Sie im Verzeichnis **Network** das Menü **Quality of Service (QoS)**.

2. Wählen Sie im Drop-down-Menü **from (Client)** die Datenquelle aus.

3. Wählen Sie im Drop-down-Menü **Service** den Dienst (Service) oder die Dienstegruppe (Service group) aus.
   Mit Ausnahme von FTP können nur Dienste ausgewählt werden, die keine Portrange enthalten.

4. Wählen Sie im Drop-down-Menü **To (Server)** das Datenziel aus.

5. Definieren Sie mit dem Drop-down-Menü **Weight** den Anteil mit dem diese Regel am Bandbreitenmanagement beteiligt ist.

   high: 3; **low**: 2; **medium**: 1

6. Definieren mit dem Drop-down-Menü **Borrow** das Verhalten dieser Regel den anderen Datenpaketen gegenüber.

   don't borrow: Dieser Datenkanal darf sich keine Bandbreite von anderen Kanälen borgen und verborgt keine Bandbreite.

   borrow: Dieser Datenkanal darf sich Bandbreite von anderen Kanälen borgen und verborgt nicht benötigte

Bandbreite. Im **Worst Case** steht allerdings die eingestellte Bandbreite zur Verfügung.

7. Übernehmen Sie die Einstellungen durch einen Klick auf die Schaltfläche **Add**.

Nach erfolgreicher Definition wird die neue **Regel** immer deaktiviert (Statusampel zeigt Rot) an letzter Stelle in die Regelsatz-Tabelle eingetragen.

Current Quality of Service Rules

In dieser Tabelle werden die übersetzten Regeln, in Reihenfolge ihres Eintreffens im Kernel, dargestellt. Diese Tabelle wird vorwiegend zur Fehlersuche des Supports benötigt.

Beispiel: Die Netzwerkkarte eth0 wurde für **QoS** freigegeben und die folgenden zwei Regeln wurden definiert:

1. Regel für Datenpakete zum NTP-Server-Atlanta

From (Client): Any
Service: NTP
To (Server): NTP_Server_Atlanta
Weight: low (2)
Borrow: don't borrow

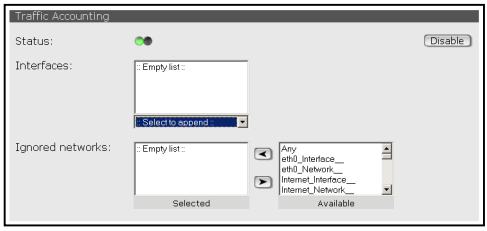
2. Regel für Datenpakete von der internen Schnittstelle etho:

From (Client): Internal_Interface__
Service: Microsoft-SQL-Server
To (Server): Private_Network_192.168.0.0
Weight: high (3)
Borrow: borrow

In der Tabelle werden alle Classes angezeigt, die für die Netzwerkkarte eth0 erstellt werden:

```
Eth0        Class 1
                    Total link bandwidth.
                    Min. BW: 100Mbit
                    Max. BW: 100Mbit

            Class 10
                    Reserved Bandwidth for unshaped
                      traffic.
                    Min. BW: 10Mbit
                    Max. BW: 100Mbit

            Class 11
                    Min. BW: 67.50Mbit
                    Max. BW: 100Mbit

                    Filter:
                    Protocol tcp
                    Protocol udp
                    Source
                      192.168.2.240/255.255.255.255
                    Destination
                    192.168.0.0/255.255.0.0
                    Destination Port 1433

            Class 12
                    Min. BW: 22.50Mbit
                    Max. BW: 22.50Mbit

                    Filter:
                    Protocol udp
                    Destination
                      130.207.244.240/255.255.255.255
                    Destination Port 123
```

5.3.8. Accounting



Mit dem **Accounting** werden auf den Netzwerkkarten alle transportierten IP-Pakete erfasst und die Datenmenge aufsummiert.
In diesem Menü können Sie spezifizieren, auf welchen Netzwerkkarten der anfallende Datenverkehr gezählt werden soll. Sie haben die Möglichkeit, die gesammelten Daten im Menü **Log Files/Accounting** herunterzuladen, oder eine tägliche Auswertung der Daten im Menü **Reporting/Accounting** zu konfigurieren.

Wichtiger Hinweis:

Im Normalfall sollte das **Accounting** nur auf einer Netzwerkkarte durchgeführt werden, da sonst weitergeleitete Datenpakete mehrmals gezählt werden.
Wenn Sie **Masquerading** verwenden, sollten Sie das **Accounting** auf der internen Netzwerkkarte durchführen. Datenpakete, die auf der externen Netzwerkkarte das Internet-Sicherheitssystem verlassen, wurden bereits auf die neue Quelladresse umgeschrieben.

Sie haben auch die Möglichkeit, **Hosts** oder **Netzwerke** vom **Accounting** auszuschließen. Nach Installation des Internet-Sicherheitssystems sind alle Netzwerke in die Accounting-Funktion einbezogen.
Netzwerk vom **Accounting** auszuschließen könnte von Interesse sein, wenn z. B. die Netzwerkkarte zur **DMZ** im **Accounting** eingetragen ist, aber ein einzelner Rechner im **DMZ** nicht mitgezählt werden soll. Da er eventuell nur für interne Zwecke genutzt wird, macht es keinen Sinn, seine Traffic-Daten in die Abrechnung einzubeziehen.

Im Menü **Reporting/Accounting** können Sie nach entsprechender Definition das **Accounting** beobachten.

Wichtiger Hinweis:

Führen Sie das **Accounting** nicht auf **Gigabit**-Netzwerkkarten aus. Durch die hohen Datenmengen kann diese Funktion sonst zu einer Auslastung des Prozessors (CPU) führen.

Netzwerkkarte hinzufügen/entfernen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Accounting**.
2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich das Fenster **Traffic Accounting**.
3. Bestimmen Sie die Netzwerkkarten mit dem Auswahlfeld **Interfaces**.

Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

Netzwerk ausschließen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Accounting**.
2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich das Fenster **Traffic Accounting**.
3. Bestimmen Sie die Netzwerke mit dem Auswahlfeld **Ignored networks**.

Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

5.3.9. Connection Tracking

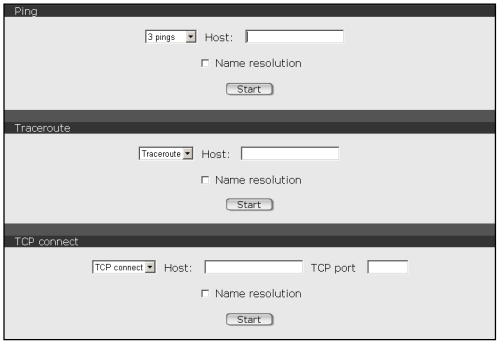
Das **Connection Tracking** ist eine interne Funktion des internet-Sicherheitssystems. In diesem Menü wird der Netzwerkdatenverkehr analysiert und eine Liste mit den gegenwärtig erstellten Verbindungen dargestellt.

In den Spalten **Source** und **Destination Address** stehen die IP-Quell- und Zieladressen der Verbindung. Falls möglich, werden auch die Hostnamen angegeben. In der Spalte **Service** wird der Quell- und der Zielport sowie der verwendete Dienst dargestellt.

Hinweis:

In diesem Menü werden nur Verbindungen mit den Protokollen TCP, UDP, GRE und ICMP dargestellt.

5.3.10. Tools



Im Menü **Tools** stehen Ihnen drei Werkzeuge zur Verfügung, mit deren Hilfe Sie die Netzwerkverbindungen und Funktionalität Ihres Internet-Sicherheitssystems testen können.

Ping und **Traceroute** dienen zur Überprüfung von Netzwerkverbindungen auf IP-Ebene. Für diese Tools muss im Menü **PACKET FILTER/ ICMP** die Funktion **ICMP on firewall** aktiviert sein. Mit **TCP Connect** können Sie TCP-Dienste auf ihre Erreichbarkeit testen.

Alle drei Tools beinhalten die Zusatzfunktion **Namensauflösung (Name Resolution)**. Sie dient dazu, dass die IP-Adressen der Antwortpakete in gültige Namen umgesetzt werden. Damit die Funktion aktiviert werden kann, muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet sein.

Ping

Mit **Ping** können Sie die Verbindung zu einem entfernten Host testen. Das Programm **Ping** verschickt an einen anderen Rechner ein **ICMP-Echo-Paket**. Wenn der Rechner das ICMP-Echo-Paket erhält, muss sein TCP-IP-Stack ein **ICMP-Echo-Reply-Paket** an den Absender zurückschicken. So können Sie feststellen, ob eine Verbindung zu einem anderen Netzwerk-Rechner möglich ist.

Hinweis:
Für das Tool **Ping** muss im Menü **PACKET FILTER/ICMP** die Funktion **ICMP on firewall** aktiviert sein.
Für die Funktion **Name Resolution** muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

Ping starten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Tools**.
2. Wählen Sie im Drop-down-Menü die Anzahl der Pings.
   Sie können wählen zwischen 3, 10 und 100 Pings.
3. Tragen Sie in das Eingabefeld **Host** die IP-Adresse oder den Namen ein.
4. Wenn Sie die Funktion **Name Resolution** aktivieren möchten, klicken Sie auf das Optionsfeld.
5. Starten Sie die Testverbindung durch einen Klick auf die Schaltfläche **Start**.

Traceroute

Traceroute ist ein Werkzeug, um Fehler beim Routing in Netzwerken zu finden. Mit diesem Tool kann der Weg zu einer IP-Adresse aufgelöst werden. Traceroute listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht nachweisbar sein, wird die Unterbrechung durch Sterne (*) angezeigt. Nach einer bestimmten Menge an Unterbrechungen wird der Versuch

abgebrochen.
Die Verbindungsunterbrechung kann viele Gründe haben, z. B. auch, dass ein Paketfilter im Netzwerkpfad kein Traceroute erlaubt.

Hinweis:
Für das Tool **Traceroute** muss im Menü **PACKET FILTER/ ICMP** die Funktion **ICMP on firewall** aktiviert sein.
Für die Funktion **Name Resolution** muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

Das Modul **Filter Live Log** wird in Kapitel 5.4.3 ab Seite 172 beschrieben.

Traceroute starten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Tools**.
2. Tragen Sie in das Eingabefeld **Host** die IP-Adresse oder den Namen ein.
3. Wenn Sie die Funktion **Name Resolution** aktivieren möchten, klicken Sie auf das Optionsfeld.
4. Starten Sie nun die Fehlersuche durch einen Klick auf die Schaltfläche **Start**.

TCP Connect

Mit dem Werkzeug **TCP Connect** können Sie TCP-Dienste auf ihre Erreichbarkeit testen.
Während auf IP-Ebene nur die Absender- und Zieladressen verwendet werden, benötigt man für TCP noch die Portnummern. Eine Verbindung auf TCP-Ebene wird aus der Absenderadresse und dem Absenderport sowie der Zieladresse und dem Zielport identifiziert.
Wenn Sie also z. B. testen wollen, ob Sie von dem Internet-Sicherheitssystem aus einen bestimmten Webserver erreichen können, müssen Sie die IP-Adresse des Webservers und Port 80 eingeben.

Hinweis:

Für die Funktion **Name Resolution** muss im Menü **Proxies/ DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

TCP Connect starten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Tools**.
2. Tragen Sie in das Eingabefeld **Host** die IP-Adresse oder den Namen ein.
3. Tragen Sie im Eingabefeld **TCP port** die entsprechende Portnummer ein.

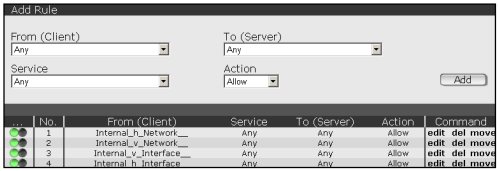
   Beispiel: Portnummer 80 für den HTTP-Dienst.
4. Wenn Sie die Funktion **Name Resolution** aktivieren möchten, klicken Sie auf das Optionsfeld.
5. Starten Sie nun die Testverbindung durch einen Klick auf die Schaltfläche **Start**.

5.4. Paketfilter (Packet Filter)

Der **Paketfilter (Packet Filter)** ist der zentrale Teil der Firewall. Über die **Paketfilterregeln** definieren Sie, welchen Datenverkehr Sie zwischen den Netzwerken/Hosts erlauben. Sie können außerdem festlegen, dass spezielle Pakete gefiltert werden und die Firewall nicht passieren dürfen.

Im Menü **Rules** setzen Sie die Paketfilterregeln und führen das Management durch. Im Menü **ICMP** schalten Sie die **ICMP**-Weiterleitung zwischen den Netzwerken ein sowie die ICMP-Nachrichten (z. B. ping) direkt zum Internet-Sicherheitssystems. In **Filter Live Log** befindet sich die Anzeige für Regelverstöße und ein Überblick über das Gesamtregelwerk (Paketfilter, NAT) auf der Firewall.

5.4.1. Rules



Im Menü **Rules** setzen Sie die Paketfilterregeln. Die Regeln werden mit Hilfe der definierten Netzwerke (**Networks**) und Dienste (**Services**) gesetzt.

Beim Einsatz von Paketfiltern unterscheidet man zwei grundlegende Arten der Security Policy:

- Alle Pakete passieren – dem Regelwerk muss ausdrücklich mitgeteilt werden, was verboten ist.
- Alle Pakete werden geblockt – das Regelwerk braucht Informationen, welche Pakete passieren dürfen.

Die Firewall dieses Internet-Sicherheitssystems ist fest auf die Variante **Alle Pakete werden geblockt** voreingestellt, da mit diesem Vorgehen eine viel höhere Sicherheit erreicht werden kann. Für den täglichen Umgang bedeutet dies, dass Sie ausdrücklich definieren, welche IP-Pakete den Filter passieren dürfen. Alle übrigen Pakete werden geblockt und anschließend im **Filter Live Log** angezeigt.

Beispiel:

Netzwerk A ist ein Sub-Netzwerk von Netzwerk B. In Regel 1 wird der Dienst SMTP für das Netzwerk A erlaubt. Regel 2 verbietet SMTP für das Netzwerk B.
Ergebnis: Ausschließlich für Netzwerk A wird SMTP erlaubt. SMTP-Pakete von allen anderen IP-Adressen aus dem restlichen Netzwerk B dürfen nicht passieren.

Eine Paketfilterregel setzt sich immer aus der Quelladresse (**From**), einem Dienst (**Service**), einer Zieladresse (**To**) und einer Maßnahme (**Action**) zusammen.

Als Quell- und Zieladresse können die folgenden Werte ausgewählt werden. Die Funktionen werden in den Kapiteln zu den entsprechenden Menüs erklärt:

- Ein Netzwerk (**Network**) - die Netzwerke werden im Menü **Definitions/Networks** definiert.
- Eine Netzwerkgruppe (**Network Group**) - die Netzwerkgruppen werden im Menü **Definitions/Network Groups** definiert.
- Ein Schnittstellen-Netzwerk (**Interface**) - diese logischen Netzwerke werden beim Konfigurieren der Netzwerkkarten und Schnittstellen vom System automatisch definiert. Die Schnittstellen werden im Menü **Network/Interfaces** konfiguriert.
- Ein **IPSec Remote Key Object**.
  Diese Adresse oder Portrange benötigen Sie, wenn Sie Paketfilterregeln für IPSec Roadwarrior Endpoints setzen möchten.

Nachdem die Paketfilterregel von Ihnen definiert wurde, wird sie deaktiviert an letzter Stelle in die Tabelle eingetragen. Die aktivierten Paketfilterregeln werden der Reihe nach von der Firewall abgearbeitet bis eine Regel zutrifft. Die Reihenfolge der Abarbeitung wird in der Tabelle **No.** angezeigt. Falls Sie die Tabelle später sortieren, z. B. nach dem Absendernetzwerk (**From (Client)**), beachten Sie bitte, dass die Anzeige der Regeln nicht mehr mit der Reihenfolge der Regelabarbeitung übereinstimmt. Falls Sie allerdings die Reihenfolge der Regeln mit der Schaltfläche **move** verändern, wird auch die Reihenfolge der Abarbeitung verändert. Falls im vorangehenden Beispiel die Regel 2 vor die Regel 1 verschoben wird, ist der Dienst SMTP für beide Netzwerke nicht mehr erlaubt. Seien Sie sehr gewissenhaft bei

der Definition dieses Regelsatzes, er bestimmt die Sicherheit der Firewall.

Wichtiger Hinweis:

Wenn eine Regel zutrifft, werden die nachfolgenden Regeln nicht mehr beachtet! Die Reihenfolge ist daher sehr wichtig. Setzen Sie nie eine Regel mit den Einträgen **Any** – **Any** – **Any** – **Allow** an die Spitze Ihres Regelwerks.

Paketfilterregel setzen:

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules**.

2. Wählen Sie im Drop-down-Menü **From (Client)** die Quelladresse der Datenpakete aus.

   Die Auswahl **Any** trifft auf alle IP-Adressen zu, egal ob es sich um offiziell zugeteilte oder private IP-Adressen gemäß RFC1918 handelt.

3. Wählen Sie im Drop-down-Menü **Service** den Dienst.

   Im Drop-down-Menü sind sowohl die vordefinierten als auch die von Ihnen selbst festgelegten Dienste enthalten. Mit Hilfe dieser Dienste lässt sich der zu bearbeitende Datenverkehr präzise definieren. Der Eintrag **Any** steht hier stellvertretend für alle Kombinationen aus Protokollen und Quell- bzw. Zielport.

4. Wählen Sie im Drop-down-Menü **To (Server)** die Zieladresse der Datenpakete aus.

   Die Auswahl **Any** trifft auf alle IP-Adressen zu, egal ob es sich um offiziell zugeteilte oder private IP-Adressen gemäß RFC1918 handelt.

5. Wählen Sie im Drop-down-Menü **Action** die Maßnahme aus, die der Paketfilter ergreift, wenn ein Paket den Einstellungen **From**, **Service** und **To** entspricht:

   Allow: Alle Pakete, die diese Bedingung erfüllen, werden durchgelassen.

   Drop: Alle Pakete, die diese Bedingung erfüllen, werden blockiert, aber nicht im **Live Log** protokolliert. Die Aktion **Drop** ist für Filterverletzungen empfehlenswert, die dauernd

stattfinden, sicherheitstechnisch nicht relevant sind und nur die Übersichtlichkeit des **Live Log** beeinträchtigen, z. B. Netbios-Broadcasts von MS Windows-Rechnern.

Log Drop: Alle Pakete, die diese Bedingung erfüllen, werden blockiert und im **Filter Live Log** als Regelverletzungen protokolliert.

Log Reject: Alle Pakete, die diese Bedingung erfüllen, werden blockiert und im **Filter Live Log** als Regelverletzungen protokolliert. Zusätzlich erhält der Absender eine entsprechende ICMP-Nachricht.

Reject: Alle Pakete, die diese Bedingung erfüllen, werden blockiert, aber nicht im **Filter Live Log** protokolliert. Zusätzlich erhält der Absender eine entsprechende ICMP-Nachricht.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Nach erfolgreicher Definition wird die neue **Paketfilterregel** immer deaktiviert an letzter Stelle in die Regelsatz-Tabelle eingetragen (Statusampel zeigt Rot).

7. Aktivieren Sie die Paketfilterregel durch einen Klick auf die Statusampel.

Anschließend stehen Ihnen zur Bearbeitung der Paketfilterregeln weitere Funktionen zur Verfügung.

Hinweis:

Neue Regeln werden per Default-Einstellung mit dem Status **Inaktiv** am Ende der Regelsatz-Tabelle erzeugt. Die Regel wird erst wirksam, wenn Sie den Status **Aktiv** vergeben.
Sehen Sie dazu **Regel aktiv/inaktiv setzen**.

Weitere Funktionen

Paketfilterregel aktiv/inaktiv setzen: Die Statusampel in der ersten Spalte zeigt den Status der Paketfilteregel an. Mit einem Klick auf die Statusampel wechseln Sie zwischen dem Status **Aktiv** (Statusampel zeigt Grün) und **Inaktiv** (Statusampel zeigt Rot).
Deaktivierte Regeln bleiben gespeichert, werden aber vom Paketfilter nicht berücksichtigt.

Paketfilterregel editieren: Durch einen Klick auf die Schaltfläche **edit** werden die Daten in das Fenster **Edit Rule** geladen. Anschließend können Sie die Eingaben bearbeiten. Durch einen Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert.
Zum Abbrechen des Vorgangs führen Sie eine beliebige andere Aktion durch (z. B. durch einen Klick auf **Rules** im Verzeichnis des WebAdmin).

Reihenfolge der Paketfilterregel ändern: Die Abfolge der Regeln in der Tabelle ist ausschlaggebend für das korrekte Funktionieren der Firewall. Durch einen Klick auf die Schaltfläche **move** können Sie die Reihenfolge der Abarbeitung verändern. Geben Sie im Eingabefeld an, vor welche Zeilennummer dieser Regelsatz verschoben werden soll und bestätigen Sie dies durch einen Klick auf die Schaltfläche **OK**.

Paketfilterregel löschen: Durch einen Klick auf die Schaltfläche **del** wird die Paketfilterregel aus der Tabelle gelöscht.

Regelsatz-Tabelle sortieren: Durch einen Klick auf die Funktion in der Kopfzeile der Regelsatz-Tabelle werden alle Regeln entsprechend sortiert. Wenn Sie z. B. die Tabelle nach den Absendernetzwerken sortieren möchten, klicken Sie auf **From (Client)**. Um die Tabelle wieder nach der Reihenfolge des **Matching** anzuzeigen, klicken Sie auf **No**.

Broadcast auf das gesamte Internet:

Um Pakete mit der Zieladresse **Broadcast-IP** zu **droppen**, muss Sie zuerst im Menü **Definitions/Networks** die entsprechende Broadcast-Adresse in Form eines neuen Netzwerks definieren. Anschließend müssen Sie die Paketfilterregel setzen und aktivieren.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks** und definieren Sie das folgende Netzwerk:

   Name: Broadcast32

   IP address: 255.255.255.255

   Subnet mask: 255.255.255.255

2. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

3. Öffnen Sie nun im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die folgende Paketfilterregel:

   From (Client): Any

   Service: Any

   To (Server): Broadcast32

   Action: Drop

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Broadcast auf ein Netzwerksegment:

Für jede im Menü **Interfaces** konfigurierte Schnittstelle wird automatisch das Netzwerk **NAME_Broadcast__** definiert.
Weitere Informationen hierzu erhalten Sie in Kapitel 5.3.1 ab Seite 104 unter der Überschrift **Current Interface Status**.

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die folgende Paketfilterregel:

   From (Client): Any

   Service: Any

   To (Server): Wählen Sie hier das Netzwerk Broadcast des entsprechenden Netzwerksegments aus.
   Beispiel: NAME_Broadcast__

   Action: Drop

2. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

5.4.2. ICMP

ICMP Settings

Hier werden die Einstellungen für **Internet Control Message Protocol (ICMP)** vorgenommen. **ICMP** ist notwendig, um die Netzwerkverbindungen und Funktionalität des Internet-Sicherheitssystems zu testen. Des Weiteren wird ICMP zur Fehlerbenachrichtigung und zu Diagnosezwecken verwendet.

Hinweis:

Nähere Informationen zu **ICMP** finden Sie auch unter **Ping** und **Traceroute**.

ICMP on firewall und **ICMP forwarding** beziehen sich immer auf alle IP-Adressen (**Any**).
Wenn diese Funktionen aktiviert sind (Statusampel zeigt Grün), können alle IPs die Firewall (**ICMP on firewall**) bzw. das Netzwerk dahinter (**ICMP forwarding**) anpingen. Einzelne IP-Adressen können dann nicht mehr mit Paketfilterregeln ausgeklammert werden.

Wichtiger Hinweis:

Die hier getroffenen Einstellungen haben stets Priorität gegenüber den Einstellungen, die im Paketfilterregelsatz definiert sind.

Wenn die **ICMP**-Einstellungen deaktiviert sind (Statusampel zeigt Rot), kann man mit geeigneten Paketfilterregeln einzelnen IPs und Netzwerken das Senden von ICMP-Paketen auf die Firewall bzw. durch die Firewall erlauben.

ICMP forwarding: Hier aktivieren und deaktivieren Sie die **ICMP**-Weiterleitung von ICMP-Paketen hinter die Firewall, d. h. ins lokale Netzwerk und alle angeschlossenen DMZs.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Wichtiger Hinweis:

Falls Sie **ICMP forwarding** deaktivieren möchten, darf im Menü **Packet Filter/Rules** keine Regel mit den Einträgen **Any** – **Any** – **Any** – **Allow** definiert sein. Das **ICMP forwarding** bleibt sonst aktiv.

ICMP on firewall: Hier aktivieren und deaktivieren Sie das direkte Senden und Empfangen von **ICMP**-Paketen. Per Default ist diese Funktion eingeschaltet (Statusampel zeigt Grün).
Mit einem Klick auf die Schaltfläche **Disable** schalten Sie die Funktion aus (Statusampel zeigt Rot).

Hinweis:

Für die Tools **Traceroute** und **Ping** muss hier die Funktion **ICMP on firewall** aktiviert sein.

Traceroute Settings

Traceroute ist ein Werkzeug, um Fehler beim Routing in Netzwerken zu finden. In diesem Fenster werden die erweiterten Einstellungen speziell für **ICMP Traceroute** vorgenommen. Zusätzlich werden die UDP-Ports für **UNIX Traceroute**-Anwendungen geöffnet.
Weitere Informationen zu **Traceroute** erhalten Sie im Kapitel 5.3.10 ab Seite 160.

Firewall is traceroute visible: Wenn diese Funktion aktiviert ist, antwortet die Firewall auf **Traceroute**-Pakete.

Firewall forwards traceroute: Wenn diese Funktion aktiviert ist, leitet die Firewall **Traceroute**-Pakete weiter.

Hinweis:

Die Funktionen **Firewall is traceroute visible** und **Firewall forwards traceroute** machen nur Sinn, wenn beide aktiviert sind.

Traceroute on firewall: Wenn diese Funktion aktiviert ist, kann der Traceroute-Befehl auf der Firewall verwendet werden.

Ping Settings

In diesem Fenster werden die erweiterten Einstellungen speziell für **ICMP Ping** vorgenommen.
Weitere Informationen zu **Ping** erhalten Sie im Kapitel 5.3.10 ab Seite 160.

Firewall is ping visible: Wenn diese Funktion aktiviert ist, antwortet die Firewall auf **Ping**-Pakete.

Firewall forwards ping: Wenn diese Funktion aktiviert ist, leitet die Firewall **Ping**-Pakete weiter.

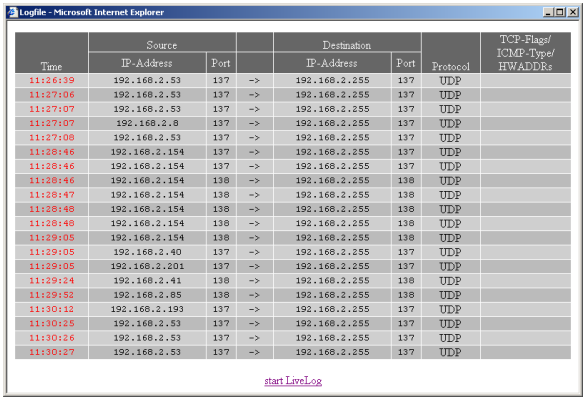
Ping on firewall: Wenn diese Funktion aktiviert ist, kann der **Ping**-Befehl auf der Firewall verwendet werden.

5.4.3. Filter Live Log

Der **Filter Live Log** dient zur Überwachung der gesetzten Paketfilter- und NAT-Regeln. Das **Packet Filter Log** zeigt in Echtzeit Pakete an, die durch den Regelsatz des Paketfilters abgefangen werden. Diese Funktion eignet sich besonders zur Fehlersuche.

Sollte nach der Inbetriebnahme des Internet-Sicherheitssystems eine Anwendung, z. B. Online-Banking, nicht verfügbar sein, können Sie anhand des **Live Log** nachvollziehen, ob und welche Pakete durch die Firewall abgefangen wurden.
Für die Ausgabefelder **Current Packet Filter rules** und **Current NAT rules** werden die aktuell gültigen Regeln direkt aus dem Betriebssystemkernel entnommen und dargestellt.

Packet Filter Logs



Time	Source IP-Address	Port		Destination IP-Address	Port	Protocol	TCP-Flags/ ICMP-Type/ HWADDRs
11:26:39	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:27:06	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:27:07	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:27:07	192.168.2.8	137	->	192.168.2.255	137	UDP	
11:27:08	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:28:46	192.168.2.154	137	->	192.168.2.255	137	UDP	
11:28:46	192.168.2.154	137	->	192.168.2.255	137	UDP	
11:28:46	192.168.2.154	138	->	192.168.2.255	138	UDP	
11:28:47	192.168.2.154	138	->	192.168.2.255	138	UDP	
11:28:48	192.168.2.154	138	->	192.168.2.255	138	UDP	
11:28:48	192.168.2.154	138	->	192.168.2.255	138	UDP	
11:29:05	192.168.2.154	138	->	192.168.2.255	138	UDP	
11:29:05	192.168.2.40	137	->	192.168.2.255	137	UDP	
11:29:05	192.168.2.201	137	->	192.168.2.255	137	UDP	
11:29:24	192.168.2.41	138	->	192.168.2.255	138	UDP	
11:29:52	192.168.2.85	138	->	192.168.2.255	138	UDP	
11:30:12	192.168.2.193	137	->	192.168.2.255	137	UDP	
11:30:25	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:30:26	192.168.2.53	137	->	192.168.2.255	137	UDP	
11:30:27	192.168.2.53	137	->	192.168.2.255	137	UDP	

Durch einen Klick auf die Schaltfläche **open live Packet Filter violation log** öffnen Sie ein neues Fenster, in dem die Regelverletzungen in der Reihenfolge ihres Auftretens in Echtzeit tabellarisch aufgelistet werden.

Durch einen Klick auf die Schaltfläche **stop Live Log**/**start Live Log** können Sie die Aktualisierung anhalten und wieder fortsetzen.

Hinweis:

Beachten Sie bitte, dass Regeln, die im Regelsatz unter **Packet Filter/Rules** mit der Aktion **Drop** und **Reject** versehen sind, nicht im **Packet Filter violation Live Log** auftauchen!

Current Packet Filter rules

Im Fenster **Current Packet Filter rules** können fortgeschrittene Administratoren in Echtzeit das Ergebnis der Filterregel-Tabelle sehen und deren Umsetzung im Kernel. Außerdem werden hier auch alle systemgenerierten Filterregeln angezeigt.

Current NAT rules

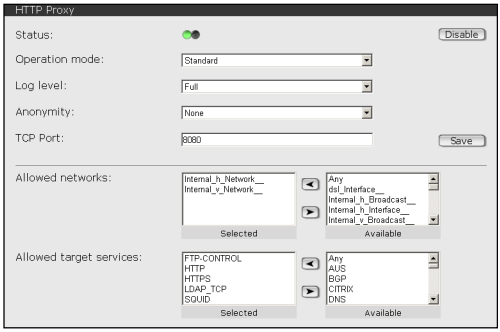
Unter **Current NAT rules** werden alle definierten und systemgenerierten NAT-Regeln aufgelistet.

5.5. Application Gateways (Proxies)

Während der **Paketfilter (Packet Filter)** auf Netzwerk-Ebene den Datenverkehr filtert, wird durch den Einsatz von **Proxies (Application Gateways)** die Sicherheit der Firewall zusätzlich auf Application-Ebene erhöht, da zwischen Client und Server keine direkte Verbindung besteht.
Jeder **Proxy** kann speziell für seinen Dienst wiederum weitere Sicherheitsdienste anbieten. Durch das Wissen jedes Proxies um den Kontext seines Dienstes ergeben sich umfangreiche Sicherungs- und Protokollierungsmöglichkeiten. Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten jeweils klar durch Protokollstandards definiert ist. Die Proxies konzentrieren sich dabei auf das Wesentliche.

Im Verzeichnis **Proxies** wählen Sie die gleichnamigen **Proxies** aus und konfigurieren die Einstellungen. Zu Beginn sind alle **Proxies** ausgeschaltet.
Die Firewall beinhaltet die Proxydienste **HTTP** (Web), **DNS** (Nameserver), **SOCKS** (Punkt-zu-Punkt-Verbindung), **POP3**, **Ident**, **SMTP** (E-Mail) und **Proxy Content Manager**.

5.5.1. HTTP/Surf Protection



Im Menü **HTTP** konfigurieren Sie die Firewall als **HTTP-Cache-Proxy**. Dieser **Proxy** ist neben dem reinen Weiterleiten von WWW-Anfragen auch in der Lage, diese Seiten zwischenzuspeichern. Häufig aufgerufene Seiten werden dann nicht mehr über das Internet neu geladen, sondern nach der ersten Übertragung nur noch aus dem Cache des Proxies abgerufen.

Hinweis:

WebAdmin kann nicht über den eigenen Proxy aufgerufen werden. Die IP-Adresse des Internet-Sicherheitssystems muss daher im Browser von der Verwendung des Proxyservers ausgeschlossen werden.

Netscape Communicator, Proxy ausschalten:

1. Öffnen Sie das Menü **Bearbeiten/Einstellungen/Erweitert/Proxies**.
2. Klicken Sie bei **Manuelle Proxies Konfiguration** auf die Schaltfläche **Anschauen**.
3. Tragen Sie in das Eingabefeld **Kein Proxy für** die IP-Adresse Ihrer Firewall ein.
4. Um die Eingaben zu speichern, klicken Sie auf die Schaltfläche **OK**.

Microsoft Explorer, Proxy ausschalten:

1. Öffnen Sie das Menü **Extras/Internetoptionen**.
2. Wählen Sie die Registerkarte **Verbindungen**.
3. Öffnen Sie das Menü **LAN-Einstellungen/Erweitert**.
4. Tragen Sie in das Eingabefeld unter **Ausnahmen** die IP-Adresse Ihrer Firewall ein.
5. Um die Eingaben zu speichern klicken Sie auf die Schaltfläche **OK**.

Der **HTTP-Proxy** setzt das HTTP-Protokoll (im Allgemeinen TCP/IP-Port 80) zur Übertragung von Webseiten um. Hierbei sollte beachtet werden, dass Teile eines Webservers, z. B. Bilder aus einer Datenbank, nicht über Port 80 abgefragt werden, sondern über einen anderen TCP-Port. Da diese Anfragen im Modus **Transparent** nicht erfasst werden, müssen sie durch eine entsprechende Regel im Menü **Packet Filter/Rules** behandelt werden.

Beispiel:

From (Client): ein lokales Netzwerk

Service: Dienst mit Zieladresse (Im Menü **Definitions/ Services** müssen Sie zuvor diesen Dienst definieren)

To (Server): IP-Adresse des Webservers oder **Any**

Action: Allow

HTTPS-Anfragen (TCP/IP-Port 443) werden unbearbeitet durch den Proxy weitergeleitet.

Hinweis:

Um den **Proxy** im Modus **Standard** verwenden zu können, muss der **Browser** entsprechend konfiguriert werden: **TCP/IP-Adresse der Firewall** und der im Menü **Proxies/HTTP** eingestellte **TCP Port**. Des Weiteren muss für den Proxydienst **HTTP** ein gültiger **Nameserver (DNS)** aktiviert sein. Ohne konfigurierten Browser kann der **Proxy** nur im Modus **Transparent** betrieben werden.

Die Betriebsmodi (Operation Mode)

Standard: Sie müssen alle Netzwerke auswählen, die in der Lage sein sollen, auf den HTTP-Proxy zuzugreifen. Alle nicht ausgewählten Netzwerke können nicht zugreifen, auch wenn der Proxy im Browser konfiguriert ist.
Ist der Proxy nicht im Browser konfiguriert, so kann durch Setzen entsprechender Regeln im Paketfilter Clients der Zugriff auf Webserver im Internet ohne Proxy ermöglicht werden.

Beispiel:

From (Client): IP-Adresse des lokalen Client

Service: HTTP

To (Server): IP-Adresse des Webservers oder **Any**

Action: Allow

Sie können den Proxy verwenden, wenn Sie die IP-Adresse Ihrer Firewall und Port 8080 konfigurieren.

Transparent: Die HTTP-Anfragen auf Port 80 aus dem internen Netzwerk werden abgefangen und durch den Proxy geleitet. Für

den Browser des Endanwenders ist dieser Vorgang völlig unsichtbar. Es entsteht kein zusätzlicher Administrationsaufwand, da für den Browser des Endanwenders keine Einstellungen geändert werden müssen.
Alle Netzwerke, die transparent weitergeleitet werden sollen, müssen im Auswahlfeld **Allowed networks** eingetragen sein. Im Modus **Transparent** ist es nicht möglich, durch etwaige Einstellungen im Browser Zugriff auf den HTTP-Proxy zu erhalten. Des Weiteren können in diesem Modus keine Daten von einem FTP-Server heruntergeladen werden. Ebenso müssen HTTPS-Verbindungen (SSL) über den Paketfilter (Packet Filter) abgewickelt werden.

User Authentication: Dieser Modus entspricht in der Funktionalität dem Modus **Standard**. Der Benutzer bekommt zusätzlich nur durch vorherige **Authentifizierung** Zugriff auf den HTTP-Proxy.

Hinweis:

Jede Änderung in **Proxies** wird ohne eine weitere Meldung sofort wirksam.

HTTP-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.
3. Wählen Sie im Drop-down-Menü **Operation mode** den Betriebsmodus aus. Beachten Sie bei den Modi die jeweils notwendige Zusatzkonfiguration.
4. Bestimmen Sie im Drop-down-Menü **Log level** den von diesem Proxy generierten Informationsumfang.

   Full: Alle Daten werden protokolliert.

   Access Log only: Nur die behandelten Daten werden protokolliert, z. B. die verwendeten URLs, die Benutzernamen und die IP-Adressen der Clients.

   None: Es werden keine Daten protokolliert.

5. Bestimmen Sie im Drop-down-Menü **Anonymity** welche Informationen aus dem Netzwerk in den HTTP-Request-Headers versendet werden.

   Standard: Nur die hier aufgeführten Header-Typen werden blockiert: Accept-Encoding, From, Referrer, Server, WWW-Authenticate und Link.

   None: Die vom Client versendeten Header werden nicht geändert.

   Paranoid: Alle Header mit Ausnahme der nachfolgend aufgezählten Typen werden blockiert. Zusätzlich wird der Header "User-Agent" geändert, so dass keine Client-Versionsinformation das Netzwerk verläßt:
   Allow, Authorization, Cache-Control, Content-Encoding, Content-Length, Content-Type, Date, Expires, Host, If-Modified-Since, Last-Modified, Location, Pragma, Accept, Accept-Language, Content-Language, Mime-Version, Retry-After, Title, Connection, Proxy-Connection und User-Agent.

   Hinweis:

   Bei der Verwendung von **Standard** oder **Paranoid** werden Cookies vom Proxy blockiert. Falls Sie Cookies benötigen, sollten Sie die Einstellung **None** verwenden.

6. Schalten Sie die Funktion **Caching** durch einen Klick auf die Schaltfläche **Enable** ein.

   Mit der Funktion **Caching** werden häufig verwendete Internetseiten im **HTTP Proxy Cache** zwischengespeichert. Per Default ist diese Funktion eingeschaltet (Statusampel zeigt Grün).

7. Tragen Sie in das Eingabefeld **TCP port** den **TCP/IP-Port** ein. Per Default ist hier bereits der TCP/IP-Port **8080** eingetragen.

8. Wählen Sie im Auswahlfeld **Allowed networks** die für diesen Proxy zugelassenen Netzwerke aus.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

9. Wählen Sie im Auswahlfeld **Allowed target services** die Dienste (Services) aus, auf die der HTTP-Proxy zugreifen

kann. Per Default sind bereits die Dienste ausgewählt, zu denen eine Verbindung als sicher gilt.

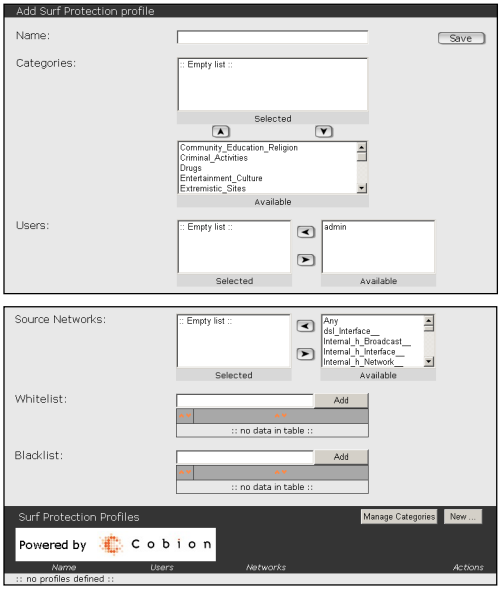
10. Falls Sie im Drop-down-Menü **Operation mode** den Modus **User Authentication** ausgewählt haben, definieren Sie nun die Methode zur Benutzerauthentifizierung.

    Authentication methods: Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **Settings/ User Authentication** konfigurier haben.

    Falls Sie die Methode **Local Users** eingestellt haben, wählen Sie nun im Auswahlfeld **Allowed users** die entsprechenden Benutzer aus. Die lokalen **Benutzer (Users)** werden im Menü **Definitions/Users** verwaltet.

11. Speichern Sie Ihre Einstellungen durch einen Klick auf die Schaltfläche **Save**.

Surf Protection Profiles



Mit der Funktion **Surf Protection Profiles** werden Profile erstellt, um den Zugriff von einem Netzwerk oder nur von einzelnen Benutzern auf bestimmte Internetseiten, abhängig von der Kategorie der **URL**, zu verhindern.
Die Kategorien basieren auf der **URL**-Datenbank von **Cobion Security Technologies**.

Dieses Modul kann erst konfiguriert werden, wenn der HTTP-Proxy eingeschaltet ist.

Surf Protection Profile konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP**.

2. Öffnen Sie durch einen Klick auf die Schaltfläche **New ...** das Menü **Add Surf Protection Profiles**.

3. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Profilnamen.
   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

4. Wählen Sie im Auswahlfeld **Categories** die Themen der Internetseiten aus, die von Ihrem System aus nicht geöffnet werden sollen.

   Die Firewall enthält bereits 17 Surf-Protection-Kategorien. Diese vordefinierten Kategorien können von Ihnen auch editiert werden.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

5. Wählen Sie in den Auswahlfeldern **Users** und **Source Networks** die Benutzer oder Netzwerke aus, die nicht auf die Internetseiten in diesem Profil zugreifen sollen.

   Hinweis:

   Die ausgewählten Benutzer (Users) werden vorrangig zu den Netzwerken (Networks) behandelt. Ein Benutzer oder Netzwerk kann immer nur einem **Surf Protection Profile** zugeordnet werden.

6. Tragen Sie in die Zugriffskontrolllisten **Whitelist** und/oder **Blacklist** die Internetadressen ein, die vom definierten Profil abweichen.

Sicherheitshinweis:

Während beim HTTP-Protokoll der Header vom **HTTP-Cache-Proxy Squid** gefiltert wird, wird dieser beim **HTTPS**-Protokoll nur durchlaufen. Das Modul **Surf Protection** kann daher bei **HTTPS**-Verbindungen keine angefragte **URL** aufgrund der **White-** oder **Blacklist** blockieren.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Blacklist: Hier können Sie zusätzlich zu den Themen im Menü **Categories** bestimmte Internetseiten angeben, die von Ihrem System aus nicht geöffnet werden sollen.

Whitelist: Hier können Sie bestimmte Internetseiten von den im Menü **Categories** gewählten Themen ausnehmen.

Beispiel: Sie haben im Auswahlfeld **Categories** das Thema **Information and Communication** ausgewählt, möchten aber den Zugriff auf die Internetseite **www.astaro.org** erlauben, dann legen Sie zusätzlich eine **Whitelist** an, indem Sie die Internetadresse in die Zugriffskontrollliste eintragen.

7. Speichern Sie nun das **Surf Protection Profile** durch einen Klick auf die Schaltfläche **Save** am Kopf des Menüs.

Nach erfolgreicher Definition wird das neue Profil immer deaktiviert an letzter Stelle in die Profil-Tabelle eingetragen (Statusampel zeigt Rot). Durch einen Klick auf die Statusampel wird das Profil aktiviert.

Wenn nun ein Benutzer oder ein Rechner aus dem definierten Profil auf eine unerlaubte Internetseite zugreift, wird der Zugang nicht nur verhindert, sondern er erhält auch eine entsprechende Meldung.

Surf Protection Categories editieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP**.

2. Öffnen Sie durch einen Klick auf die Schaltfläche **Manage Categories** das Menü **Surf Protection Categories**.

In der Tabelle **Surf Protection Categories** werden die Namen der Kategieren und die darin enthalten Unterkategorien angezeigt. In Klammer wird die Anzahl der vorhanden Kategorien angezeigt.

3. Klicken Sie bei der Kategorie die Sie editieren möchten auf die Schaltfläche **edit**.

   Anschließend öffnet sich das Fenster **Edit Category**.

4. Editieren Sie mit dem Auswahlfeld die Kategorie. Die Änderung wird sofort übernommen und in der Tabelle bei der entsprechenden Kategorie angezeigt.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

5. Klicken Sie nach Durchführung der Änderungen auf die Schaltfläche **Close**.

Anschließend wird das Fenster **Edit Category** geschlossen.

Content Filter

In diesem Fenster können Sie bestimmte Komponenten von Internetseiten auswählen, die bei Anfragen aus Ihrem System grundsätzlich geblockt werden sollen.

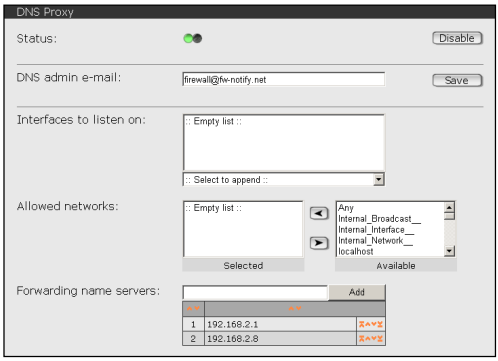
Wählen Sie die Komponenten durch einen Klick auf die Optionsfelder aus und speichern Sie anschließend die Auswahl durch einen Klick auf die Schaltfläche **Save**.

Clear Cache

Häufig aufgerufene Seiten werden nicht mehr über das Internet neu geladen, sondern nach der ersten Übertragung nur noch aus dem **HTTP Proxy Cache** abgerufen.

In diesem Fenster können Sie den Inhalt des Caches durch einen Klick auf die Schaltfläche **Start** löschen.

5.5.2. DNS



Mit dem **DNS-Proxy** können Sie den Clients in Ihrem System **Nameserver**–Dienste zur Verfügung stellen. Wenn Sie mehrere Nameserver angeben, werden die Server in Reihenfolge ihrer Eingabe bei der Auflösung von Rechnernamen befragt.

Wenn kein Nameserver im Menü **Forwarding name servers** eingetragen ist, werden alle Nameserver-Anfragen an die Internet-ROOT-Nameserver geschickt. Falls Ihr Internet Service Provider oder Sie selbst einen Nameserver betreiben, sollte dieser eingetragen sein. Abfragen an diesen lokalen Nameserver sind immer schneller als Anfragen an die ROOT-Nameserver.
Die ROOT-Nameserver sind ein fester Bestandteil des Internets. 15 ROOT-Nameserver sind weltweit verteilt und bilden die Ur-Instanz für alle untergeordneten Nameserver.

Tipp:

Selbst wenn Sie den DNS-Proxy nicht benutzen möchten, ist es sinnvoll die Nameserver Ihres Internet Service Providers als Forwarder zu konfigurieren. Diese werden dann auch bei abgeschaltetem Proxy von der Firewall selbst verwendet. Damit wird zur Entlastung des Root Nameservers beigetragen und die Firewall erzeugt nur lokale Anfragen, die in der Regel schneller beantwortet werden.

DNS-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **DNS**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.
3. Tragen Sie in das Eingabefeld **DNS admin e-mail** die E-Mail-Adresse des DNS-Administrators ein. Die E-Mail-Adres-

se wird für die syntaktisch korrekte Konfiguration benötigt und zeigt den Maintainer des DNS-Proxy an.

4. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

5. Konfigurieren Sie den **DNS-Proxy**:

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

   Interfaces to listen on: Wählen Sie die Netzwerkkarte aus, über die der DNS-Proxy erreichbar sein soll. In der Regel ist dies die interne Netzwerkkarte.
   Die Netzwerkkarten werden im Menü **Network/Interfaces** konfiguriert. Die Konfiguration einer Netzwerkkarte bzw. Schnittstelle wird in Kapitel 5.3.1 ab Seite 104 beschrieben.

   Allowed networks: Wählen Sie die für diesen Proxy zugelassenen Netzwerke aus.

   Sicherheitshinweis:

   Wählen Sie im Menü **Allowed networks** möglichst nicht **Any** aus. Der **DNS-Proxy** kann sonst von allen Internet-Teilnehmern genutzt werden.

   Forwarding nameservers: Tragen Sie in das Eingabefeld die IP-Adresse des Nameservers ein.
   Neue Adressen werden vom Eingabefeld durch einen Klick auf die Schaltfläche **Add** in das Hierarchiefeld übernommen.

   Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten.

5.5.3. SOCKS

SOCKS ist ein universeller Proxy, der von vielen Client-Applikationen unterstützt wird. Einige Beispiele dafür sind Instant Messaging Clients wie ICQ oder AIM, FTP-Clients und RealAudio. SOCKS kann stellvertretend für Clients TCP-Verbindungen aufbauen und als Besonderheit auch eingehende Verbindungen mit dem TCP- oder UDP-Protokoll annehmen (listening). Das macht SOCKS besonders auf Firewalls interessant, die NAT benutzen, da SOCKS die Nachteile von NAT ausgleichen kann. Die SOCKS-Implementation dieser Firewall unterstützt die Protokollversionen SOCKSv4 und SOCKSv5.
Bei Verwendung des SOCKSv4-Protokolls ist keine **Benutzerauthentifizierung (User Authentication)** möglich.

Hinweis:

Wenn Sie diesen Proxy verwenden möchten, um Host-Namensauflösung in SOCKS5 zu betreiben, müssen Sie auch den DNS-Proxy aktivieren.

SOCKS-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **SOCKS**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.
3. Konfigurieren Sie den **SOCKS-Proxy**:

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

   Allowed networks: Hier wählen Sie die für diesen Proxy zugelassenen Hosts und Netzwerke aus.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten.

SOCKS-Proxy mit Benutzerauthentifizierung:

Wenn Sie für den SOCKS-Proxy die Funktion **User Authentication** einschalten, müssen sich die Benutzer mit Benutzernamen und Passwort anmelden. Da **User Authentication** nur mit SOCKSv5 funktioniert, ist die Protokollversion SOCKSv4 dann nicht verfügbar.

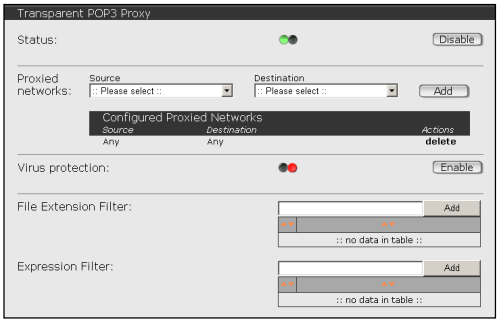
Mit dem Auswahlfeld **Authentication methods** bestimmen Sie die Methode zur Benutzerauthentifizierung. Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **Settings/User Authentication** konfigurier haben. Wenn Sie als Methode **Local Users** auswählen, können Sie für lokale Benutzer festlegen, ob sie den **SOCKS-Proxy** benutzen dürfen.
Die lokalen **Benutzer (Users)** werden im Menü **Definitions/ Users** verwaltet.

5.5.4. POP3

POP3 ist die Abkürzung für **Post Office Protocol 3** und ist ein Protokoll um E-Mails von einem Mail-Server zu empfangen. Das Gegenstück zu POP3 ist das Protokoll **SMTP**. SMTP steht für Simple Mail Transfer Protocol. Mit Diesem Protokoll werden E-Mails über einen Mail-Server versendet.

In diesem Menü konfigurieren Sie den **POP3-Proxy** für eingehende E-Mails. Der POP3-Proxy arbeitet im Transparentmodus. Die POP3-Anfragen auf Port 110 aus dem internen Netzwerk werden abgefangen und durch den Proxy geleitet. Für den Client ist dieser Vorgang völlig unsichtbar. Es entsteht kein zusätzlicher Administrationsaufwand, da am Client des Endanwenders keine Einstellungen geändert werden müssen.

POP3-Proxy konfigurieren:



In der Regel muss der POP3-Proxy nur eingeschaltet werden, da per Default bereits festgelegt ist, dass die POP3-Anfragen aus allen Netzwerken durch den Proxy geleitet werden. Die entsprechende Einstellung wird in der Tabelle **Configured Proxied Networks** angezeigt.

Falls POP3-Anfragen nur aus bestimmten Netzwerken weitergeleitet werden sollen, muss die Konfiguration geändert werden. Beachten Sie dabei, dass in den Drop-down-Menüs nur die Netzwerke zur Verfügung stehen, die zuvor im Menü **Definitions/Networks** definiert wurden.

Beispiel: POP3-Anfragen aus dem Sub-Netzwerk `192.168.0.0/255.255.0.0` an `pop.yoursite.com` sollen durch den Proxy geleitet werden. Diese Netzwerke müssen zuerst im Menü **Networks** definiert werde. Anschließend gehen Sie wie folgt vor:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **POP3**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

3. Definieren Sie im Fenster **Proxied Networks** aus welchen Netzwerken POP3-Anfragen vom Proxy weitergeleitet werden sollen.

   Source: Wählen Sie hier die Quelladresse aus.
   Beispiel: Name des Netzwerks `192.168.0.0/255.255.0.0`

   Destination: Wählen Sie hier die Zieladresse aus.
   Beispel: Name des Netzwerks `pop.yoursite.com`

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

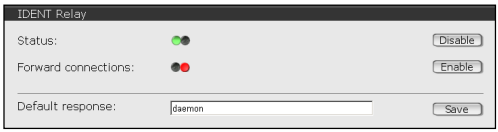
Virus Protection: Mit dieser Funktion werden E-Mails und Anhänge (Attachments) auf gefährliche Inhalte, z. B. Viren und Trojanische Pferde untersucht. Der Scanvorgang wird im E-Mail-Header vermerkt.

Wenn das Modul **Virus Protection** eingeschaltet ist, werden die gefilterten E-Mails im Menü **Proxies/Proxy Content Manager** angezeigt.

File Extension Filter: Mit diesem Modul filtert die Firewall die Anhänge (Attachments) mit den Erweiterungen aus der Kontrollliste.

Expressions Filter: Es besteht auch die Möglichkeit, dass neue Viren der Firewall noch nicht bekannt sind. Diese Viren können aber auch aufgrund einer bekannten Zeichenkette, z. B. der I-love-you-Virus, erkannt werden. Die Zeichenketten werden in dieses Modul eingegeben. Wenn nun eine E-Mail diese Zeichenkette enthält, wird sie blockiert.

5.5.5. Ident



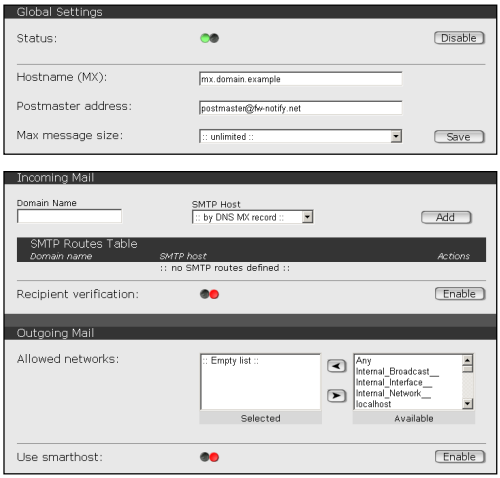
Das **Ident**-Protokoll wird von einigen Servern zur einfachen Indentitätsüberprüfung der zugreifenden Clients verwendet. Obwohl dieses Ident-Protokoll unverschlüsselt ist, verwenden es noch viele **Dienste** (**Services**) und setzen es manchmal sogar voraus.

Dieses Internet-Sicherheitssystem unterstützt zur Beantwortung Ident-Anfragen, wenn Sie die Funktion **Ident** einschalten. Das System wird immer mit dem String antworten, den Sie als **Default Response** definieren, unbeachtet dessen von welchem lokalen Dienst diese Verbindung gestartet wurde.

Forward Connection

Die Ident-Anfragen werden vom **Connection Tracking** nicht erkannt. Dies kann umgangen werden, wenn Sie die Funktion **Masquerading** verwenden. Mit **Forward Connection** können Sie die Ident-Anfragen an einen mit **Masquerading** verborgenen Host hinter die Firewall weiterleiten.
Beachten Sie dabei, dass die aktuelle IP-Verbindung nicht übergeben wird. Stattdessen wird die Firewall beim internen Client nach einer Ident-Antwort anfragen und diesen String an den externen Server weiterleiten. Dieses Vorgehen wird von den meisten Mini-Ident-Servern unterstützt, der meist Bestandteil der heute gängigen IRC- und FTP-Clients ist.

5.5.6. SMTP



Mit dem **SMTP-Proxy** schützen Sie den internen Mail-Server vor Angriffen. Ein- und ausgehende E-Mails werden auf schädliche Inhalte überprüft. Sie können in diesem Menü auch Antispam-Parameter eingeben, um unerwünschte E-Mails zu filtern.

In diesem Menü konfigurieren Sie den **SMTP-Proxy** für E-Mails. Der SMTP-Proxy empfängt alle E-Mails auf dem Gateway und versendet Sie im zweiten Prozess wieder. Damit werden keine Protokollbefehle weitergeleitet, sondern nur die Daten selbst. Der SMTP-Proxy setzt das SMTP-Protokoll auf dem TCP/IP-Port 25 um.

Hinweis:

Um eine einwandfreie Funktion des **SMTP**–Relay zu gewährleisten, muss ein gültiger **Nameserver (DNS)** aktiviert sein. Die Firewall-Benachrichtigungen an den Administrator werden auch bei abgeschaltetem **SMTP-Proxy** verschickt.

Sicherheitshinweis:

Von der Firewall werden, um **Denial of Service (DoS)**-Attacken vorzubeugen, bis zu 25 gleichzeitig eingehende SMTP-Verbindungen bearbeitet. Die 26. einkommende Verbindung wird nicht mehr angenommen.

SMTP-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **SMTP**.

2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

3. Führen Sie im Fenster **Global Settings** die Grundeinstellungen durch.

   Hostname (MX): Tragen Sie hier den Hostnamen ein.

   Wichtiger Hinweis:

   Wenn Sie TLS-Verschlüsselung verwenden möchten, muss dieser Hostname identisch sein mit dem in Ihrer DNS-Zone angegebenen **MX Record** (Mail Exchanger). Ansonsten werden andere SMTP-Server eventuell die Auslieferung von E-Mails mit TLS verweigern.

   Postmaster address: Geben Sie hier die E-Mail-Adresse des Postmasters ein.

   Max message size: Hier stellen Sie die maximale Dateigröße für die ein- und ausgehenden E-Mails ein. Übliche Werte sind 20 oder 40 MB.
   Bitte beachten Sie, dass durch die Kodierungsverfahren an E-Mails angehängte Dateien wesentlich größer werden können.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **Save**.

5. Definieren Sie nun im Fenster **Incoming Mail** die Route für die eingehenden E-Mails.

   Domain Name: Damit E-Mails für eine bestimmte Domain entgegengenommen werden können, muss der Name der Domain angegeben werden (z. B. meinedomain.com).

   SMTP Host: Alle E-Mails für diese Domain müssen an einen bestimmten Host weitergeleitet werden. Übliche Hosts sind in diesem Fall z. B. der **Microsoft-Exchange-Server** oder **Lotus Notes**. Der Host muss zuvor im Menü **Definitions/ Networks** definiert werden.
   Sie können auch definieren, dass E-Mails an die angegebene Domain durch den MX-Record zugeschickt werden. Jedoch

müssen Sie zuvor sicherstellen, dass die Firewall-IP-Adresse nicht selbst der primäre MX-Record der Domain ist, da sie keine E-Mails an sich selbst verschicken wird.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Recipient Verification: Der Proxy akzeptiert eingehende E-Mails erst nachdem die jeweilige Empfängeradresse von dem oder den Mail-Server/n bestätigt wurde. Dies hat zur Folge, dass der Umfang an Spam-Mails drastisch gesenkt wird, da E-Mails an ungültige Zieladressen nicht mehr angenommen werden.
   Voraussetzung für diese Funktion ist, dass der jeweilige Mail-Server die E-Mails an unbekannte Adressen auf SMTP-Ebene zurückweist. Die Grundregel ist: Wenn der Mail-Server die E-Mail zurückweist, dann wird auch die Firewall diese zurückweisen.

7. Wählen Sie nun im Fenster **Outgoing Mail** die Netzwerke oder Hosts aus, die in der Lagen sein sollen, über den **SMTP-Proxy** E-Mails zu versenden.

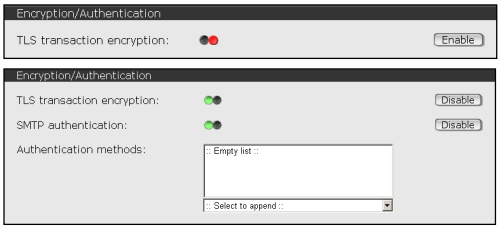
   Sicherheitshinweis:

   Die Nachrichten, die von diesen Netzwerken aus abgeschickt werden, werden von Spam Detection nicht gescant.

   Use Smarthost: Wenn Sie zum Versenden von E-Mails einen **Upstream Smarthost** verwenden möchten, schalten Sie diese Funktion ein und tragen den Hostnamen oder die IP-Adresse in das Eingabefeld ein. Der Proxy stellt in diesem Fall die E-Mails nicht selbst zu, sondern schickt alles an den Smarthost. Dies gilt allerdings nicht für E-Mails, deren Domain im Fenster **Incoming Mail** definiert sind.

   Für den Smarthost können optional noch **Benutzername** (**Username**) und **Passwort** (**Password**) definiert werden.

Encryption/Authentication



Mit der Funktion **TLS Transaction Encryption** werden alle ein- und ausgehenden E-Mails automatisch stark verschlüsselt. Voraussetzung ist, dass der externe Host diese Funktion unterstützt. TLS wird auf der Firewall nur zur Verschlüsselung eingesetzt, nicht zur Authentifizierung. SMTP ist normalerweise unverschlüsselt und kann von Dritten leicht mitgelesen werden. Die Funktion sollte aus diesem Grund möglichst eingeschaltet werden.

Wichtiger Hinweis:

Einige Mail-Server, z. B. Lotus Domino, haben teilweise Fehler in ihrer **TLS**-Konfiguration. Diese Mail-Server kündigen beim Verbindungsaufbau TLS an, obwohl sie durch eine unvollständige Konfiguration nicht in der Lage sind, eine TLS-Sitzung aufzubauen. Wenn TLS eingeschaltet ist, können keine E-Mails an diese Server verschickt werden. Bitte kontaktieren Sie in solch einem Fall die Administratoren dieser Mailserver.

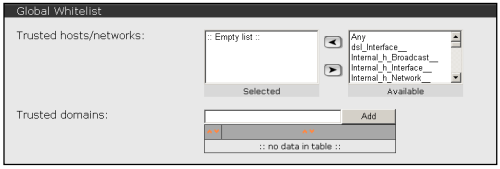
Wenn die Funktion **TLS Transaction Encryption** aktiviert ist, können Sie auch **SMTP Authentication** einschalten. Mail-Clients, z. B. Microsoft Outlook, Outlook Express oder Netscape Messenger können sich dann am **SMTP-Proxy** authentifizieren. Dies ist für dynamische IP-Endpunkte, die nicht im Menü **Outgoing Mail** definiert werden können, sehr nützlich.

Bitte verwenden Sie in den SMTP-Authentifizierungseinstellungen des Clients nicht die Funktion SPA (Secure Password Authentication). Dies ist eine alternative Verschlüsselungsmethode, die von der Firewall nicht unterstützt wird. Verwenden Sie stattdessen eine unverschlüsselte Authentifizierungsmethode, und schalten zusätzlich für ausgehende E-Mails das TLS (oder SSL) Protokoll ein.

Mit dem Auswahlfeld **Authentication methods** bestimmen Sie die Methode zur Benutzerauthentifizierung. Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **Settings/User Authentication** konfigurier haben.

Die lokalen **Benutzer (Users)** werden im Menü **Definitions/ Users** verwaltet.

Global Whitelist



Trusted Hosts/Networks: In dem Auswahlfeld kann eine **Global Wightlist** mit vertrauenswürdigen Hosts oder Netzwerken definiert werden, die in diesem Fall von den folgenden Optionen ausgeschlossen werden:

- Realtime Blackhole Lists
- Sender Verification
- MIME Error Checking
- Spam Detection
- Expression Filter

Dies hat zur Folge, dass die benötigte Rechenleistung für Scanvorgänge herabgesetzt wird und dass problematische Hosts vom Content Scanning ausgeschlossen werden können.

Trusted Domains: In der Hierarchieliste kann eine **Global Wightlist** mit vertrauenswürdigen Domain-Namen definiert werden.

Sicherheitshinweis:

Diese Funktion sollte allerdings nur mit Vorsicht eingesetzt werden, da Absenderadressen auch leicht gefälscht werden können.

5.5.6.1. Antispam/Content Control

Block RCPT Hacks

Der Proxy akzeptiert keine E-Mails die eine Absenderadresse mit den Zeichen **!**, **%**, **/**, **|** oder einem zusätzlichen **@** enthält. Des Weiteren werden auch E-Mails nicht akzeptiert, die mit einem **Dot** (**.**) beginnen.

Realtime Blackhole Lists (RBL)

Mit dem Modul **RBL** können externe Datenbanken mit den ihnen bekannten Spam-Hosts abgefragt werden. Im Internet werden mehrere Dienste dieser Art angeboten. Durch diese Funktion kann der Umfang an unerwünschten E-Mails stark reduziert werden.

Einen kommerziellen Dienst finden Sie unter der Internetadresse http://www.mail-abuse.org.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine gefilterte E-Mail behandelt wird, die von einer der aufgeführten Domains abgeschickt wurde. Folgende Aktionen sind möglich:

- **Warn**: Wenn eine E-Mail von einer Domain abgesendet wurde, die in einer der Datenbanken in der Kontrollliste **Zone** enthalten ist, wird ihr der Header **X-RBL-Warning** hinzugefügt. Die verschiedenen Header wird in der Beschreibung zum Modul **Spam Detection** erklärt.
- **Reject**: Die E-Mails, die von einer Domain aus der Datenbank in er Kontrollliste zugesendet wurden, werden nur zurückgewiesen.
- **Zone**: Tragen Sie in die Kontrollliste die Adressen der Datenbanken ein.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Sender Address Verification

Mit dieser Funktion werden die Absenderadressen von eingehenden E-Mails überprüft. Es wird geprüft, ob die Domain des Absenders existiert. Falls die Domain nicht existiert, wird die E-Mail zurückgewiesen.
Wenn zusätzlich die Funktion **Callout** eingeschaltet ist nimmt der Proxy Verbindung zum SMTP Relay des Absenders auf und prüft durch einen RCPT-Befehl, ob der Absender von diesem Server akzeptiert wird. Sollte dies nicht der Fall sein, wird der Proxy keine E-Mails von dieser Adresse mehr annehmen.

Sender Blacklist

Mit dieser Funktion können E-Mails von bestimmten Absenderadressen, z. B. von bekannten Spam-Hosts geblockt werden. Beide Absenderadressen auf dem Umschlag sowie die From- und Reply-To-Header der eingehenden E-Mails werden mit der Kontrollliste verglichen.

Tragen Sie die E-Mail-Adressen wie nachfolgend beschrieben in die Kontrollliste **Patterns** ein:

- E-Mails einer bestimmten Adresse sollen geblockt werden.
  Eingabe: user@domain.com
- Alle E-Mails einer bestimmten Domain sollen geblockt werden.
  Beispiel: *@domain.com
- Alle E-Mails eines bestimmten Benutzers sollen blockiert werden, egal von welcher Domain diese abgesendet werden.
  Beispiel: user@*

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Wenn die Firewall nun eine E-Mail von einer Adresse aus der Kontrollliste empfängt, wird diese mit der Fehlermeldung **5xx** und dem Kommentar **Your address (envelope or header) is blacklisted at this site** zurückgesendet.

MIME Error Checking

Die Funktion **MIME Error Checking** kann Fehler in Nachrichten erkennen, die mit **MIME** verschlüsselt wurden. **MIME** steht für **M**ultipurpose **I**nternet **M**ail **E**xtensions. MIME legt die Struktur und den Aufbau von E-Mails und anderer Internetnachrichten fest. Es ist eine Kodierungsvorschrift, die den Versand von Nicht-Text-Dokumenten, wie Bilder, Audio und Video in textbasierten Übertragungssystemen ermöglicht. Die Nicht-Text-Elemente werden beim Versender verschlüsselt und beim Empfänger wieder entschlüsselt.

Die Funktion **MIME Error Checking** kann dabei helfen Angriffe, bei denen die Fehler-Toleranzabweichung in der MIME-Entschlüsselungs-Software ausgenutzt werden zu erkennen.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlernummer **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** als Typ **SMTP_ERR** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.
- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

Trigger on: In diesem Drop-down-Menü legen Sie fest, welche Fehler dazu führen, dass die E-Mail laut Funktion Action behandelt wird:

- **Level 1**: Diese Stufe bewirkt, dass nur die E-Mails mit den schwersten Fehlern behandelt werden. Diese Einstellung wird

empfohlen, da viele Anwender ein fehlerhaftes Verschlüsselungsprogramm verwenden, das bei den höheren Stufen (Level 2 und 3) bereits anspricht.

- **Level 2**: Mit Ausnahme der mit alltäglichen Fehlern behafteten E-Mails, werden alle behandelt.
- **Level 3**: Alle E-Mails mit Fehlern werden behandelt.

File Extension Filter

Mit diesem Modul filtert die Firewall die Anhänge (Attachments) mit den Erweiterungen aus der Kontrollliste **Extensions**.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** als Typ **SMTP_ERR** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zurückzusenden.
- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

Extensions: Tragen Sie in die Kontrollliste alle Dateierweiterungen, z. B. **exe** ein, die von der Firewall gefiltert werden sollen.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Virus Protection

Mit dieser Funktion werden E-Mails und Anhänge (Attachments) auf gefährliche Inhalte, z. B. Viren und Trojanische Pferde untersucht. Der Scanvorgang wird im E-Mail-Header vermerkt.

Falls **Virus Protection** eine infizierte E-Mail entdeckt, wird diese von der Firewall gefiltert. Die weitere Behandlung der E-Mail hängt von der Einstellung im Drop-down-Menü **Action** ab.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** als Typ **SMTP_ERR** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen.
- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

Spam Detection

Dieses Modul überprüft die eingehenden E-Mails heuristisch auf bestimmte Eigenschaften die Hinweise auf Spam geben. Hierzu dienen interne Musterdatenbanken. Auf diese Weise ist man unabhängig von den Absenderinformationen und kann somit die Genauigkeit stark erhöhen.

Für den Spam Score können zwei **Grenzwerte** (**Thresholds**) definiert werden. Auf diese Weise können mutmaßliche SPAM E-Mails von der Firewall unterschiedlich behandelt werden.
Die beiden **Grenzwerte** (**Thresholds**) sind gleichberechtigt. Der

Grenzwert mit der höheren Stufe sollte allerdings strenger behandelt werden.

Default-Einstellungen:

Grenzwert Eins (**Threshold One**)

When Spam Level exceeds: 03 (aggressive),
do this: Pass.

Grenzwert Zwei (**Threshold Two**)

When Spam Level exceeds: Keine Einstellung,
do this: Keine Einstellung.

Der erste Grenzwert hat zur Folge, dass E-Mails ab Stufe 3 gefiltert, aber durchgelassen werden. Mit Hilfe des hinzugefügten Headers kann die E-Mail auf dem Mail-Server oder im E-Mail-Programm des Empfängers sortiert oder gefiltert werden.

Grundsätzliche gilt, dass der **Grenzwert** (**Threshold**) mit der höheren Stufe eine strengere Behandlung (**do this**) erfahren soll.

Wichtiger Hinweis:

Das Modul **Spam Detection** benötigt auf stark frequentierten Systemen einen hohen Anteil der Systemressourcen.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlernumer **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** als Typ **SMTP_ERR** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zurückzusenden.

- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern. Des Weiteren wird in den Betreff des E-Mails der Hinweis **SPAM** hinzugefügt.

Strategy: Mit diesem Drop-down-Menü justieren Sie den Höchstwert zur Bewertung der E-Mails. Der Unterschied zwischen den Höchstwerten definiert sich auch durch die Wahrscheinlichkeit, dass ungefähliche Mails, z. B. HTML-Newsletter gefiltert werden. Die Folgenden drei Strategien sind möglich:

- **Aggressive**: Diese Strategie filtert die meisten Spam-Mails. Allerdings werden mit hoher Wahrscheinlichkeit auch ungefährliche Nachrichten, z. B. HTML-Newsletter zurückgewiesen.
- **Reasonable**: Diese Strategie ist per Default voreingestellt und liegt zwischen **Aggessive** und **Reasonable**.
- **Conservative**: Diese Strategie filtert nur Nachrichten, bei denen es sich mit sehr hoher Wahrscheinlichkeit um Spam-Mails handelt. Ungefährliche E-Mails werden meist nicht gefiltert.

Spam sender whitelist: Diese Kontrollliste kann nur für das Modul **Antispam** definiert werden. Tragen Sie in die Liste die E-Mail-Adressen der Absender ein, deren Nachrichten nicht gefiltert werden sollen.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

Die Header:

Es gibt viel Funktionen bei denen der Nachricht ein **Header** hinzugefügt wird. Dieser Header soll den Benutzer über spezielle Eigenschaften dieser Nachricht informieren. Wenn nun in der entsprechenden Funktion **Pass** ausgewählt wird, können die Empfänger die Nachrichten mit ihrer E-Mail-Software sortieren oder filtern. In der nachfolgenden Liste sind alle Header enthalten, die der HTTP-Proxy an die E-Mails hinzufügen kann:

- **X-Spam-Score**: Dieser Header wird vom Modul **Spam Detection** hinzugefügt. Er enthält einen Punktestand, der aus einem numerischen Wert und einer Anzahl von Minus- und Pluszeichen besteht. Je höher dieser Punktestand ausfällt, umso wahrscheinlicher ist es, dass es sich bei der Nachricht um eine Spam-Mail handelt.

Wenn Sie im Modul **Spam Detection** die Aktion **Pass** auswählen, kann der Empfänger die E-Mail mit seiner E-Mail-Software filtern.

- **X-Spam-Flag**: Wenn der enthaltene Wert **Yes** lautet, wurde die Nachricht als Spam-Mail erkannt.
- **X-Spam-Report**: Der Proxy hat die Nachricht als Spam-Mail erkannt. Der hinzugefügte Multiline Header enthält einen offen lesbaren Antispam-Bericht.
- **X-Infected**: Die Nachricht enthält einen Virus. Als Wert wird der Name des gefundenen Viruses angezeigt.
- **X-Contains-File**: Das Modul **File Extension Filter** ist eingeschaltet und eine E-Mail enthält einen oder Anhang (Attachment) mit einer Erweiterung aus der Kontrollliste.
- **X-Regex-Match**: Das Modul **Expression Filter** ist eingeschaltet und das E-Mail beinhaltet eine Zeichenkette aus der Kontrollliste.
- **X-RBL-Warning**: Das Modul **Realtime Blackhole Lists (RBL)** ist eingeschaltet und die E-Mail wurde von einer Domain abgeschickt, die in der Kontrollliste **Zones** enthalten ist. Dieser Header wird der Nachricht hinzugefügt, wenn im Drop-down-Menü **Action** die Funktion **Warn** ausgewählt ist.

Expression Filter

Es besteht auch die Möglichkeit, dass neue Viren der Firewall noch nicht bekannt sind. Diese Viren können aber auch aufgrund einer bekannten Zeichenkette, z. B. der I-love-you-Virus, erkannt werden. Die Zeichenketten werden in dieses Modul eingegeben. Wenn nun eine E-Mail diese Zeichenkette enthält, wird sie blockiert.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Mana-**

ger als Typ **SMTP_ERR** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zurückzusenden.

- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

Expressions: Tragen Sie in die Kontrollliste die Zeichenketten ein.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.4 ab Seite 37 beschrieben.

In Microsoft Outlook 2000 Regeln erstellen:

In **MS Outlook** können die von der Firewall gefilterten und anschließend durchgelassenen E-Mails sortiert werden. Voraussetzung hierfür ist, dass im Drop-down-Menü **Action** der entsprechenden Module auf der Firewall die Funktion **Pass** ausgewählt wurde.

1. Starten Sie **MS Outlook**.
2. Klicken Sie auf **Posteingang**.
3. Öffnen Sie das Menü **Extras/Regel-Assistent**.
4. Klicken Sie auf die Schaltfläche **Neu**.

   Anschließend öffnet sich der Assistent zur Erstellung neuer Regeln. Dieser Regel-Assistent führt Sie nun schrittweise durch die Konfiguration.
5. Welche Art von Regel möchten Sie erstellen? (Schritt 1)

   Wählen Sie die Regel **Nachricht bei Ankunft prüfen** aus.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.
6. Welche Bedingung(en) möchten Sie überprüfen? (Schritt 2)

   Wählen Sie in diesem Fenster die Bedingung **mit bestimmten Wörtern in der Nachrichtenkopfzeile** aus.

   Klicken Sie im Fenster **Regelbeschreibung** auf den unterstrichenen Textabschnitt und tragen Sie in das Eingabefeld

Text suchen den Namen des Headers ein.
Beispiel: **X-Spam-Score**

Klicken Sie anschließend auf die Schaltfläche **Weiter**.

7. Was soll mit dieser Nachricht passieren? (Schritt 3)

   Definieren Sie in diesem Fenster, was mit der gefilterten E-Mail passieren soll. Falls z. B. die gefilterten E-Mails in einen bestimmten Zielordner verschoben werden sollen, wählen Sie die Aktion **diese in den Ordner Zielordner verschieben** aus.

   Durch einen Klick auf **Zielordner** im Fenster **Regelbeschreibung** öffnet sich ein neues Menü. Hier können Sie entweder einen vorhanden Ordner auswählen oder einen neuen Zielordner für die gefilterten E-Mails erstellen.
   Beispiel: **Spam**
   Speichern Sie in diesem Menü die neuen Einstellungen durch einen Klick auf die Schaltfläche **OK**.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

8. Ausnahme hinzufügen (Schritt 4)

   Das Modul **Spam Detection** überprüft eingehende E-Mails heuristisch auf bestimmte Eigenschaften. Daher kann es vorkommen, dass auch ungefährliche Nachrichten, z. B. HTML-Newsletter, gefilteret werden. In diesem Menü können Sie Ausnahmen definieren und so E-Mails, z. B. Nachrichten eines bestimmten Absenders, von dieser Regel ausschließen.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

9. Geben Sie einen Namen für die Regel ein (Schritt 5)

   Tragen Sie in das Eingabefeld einen eindeutigen Namen für diese Regel ein. Mit den darunter liegenden Optionsfeldern können Sie diese Regel **aktivieren** und auch auf E-Mails anwenden, die sich bereits im Ordner **Posteingang** befinden. Im Fenster Regelbeschreibung können Sie Ihre Einstellungen ändern.

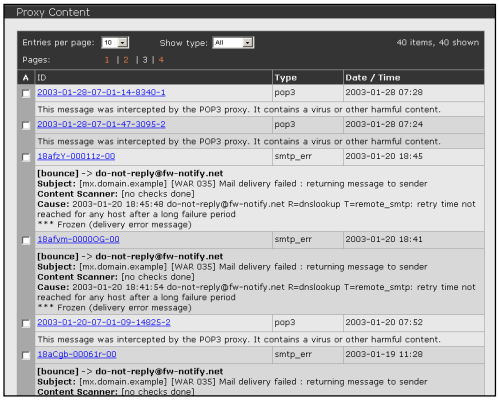
   Klicken Sie anschließend auf die Schaltfläche **Fertig stellen**.

10. Regeln in dieser Reihenfolge anwenden (Schritt 6)

Im Regel-Assistenten können Sie die Regeln durch einen Klick auf das Optionsfeld aktivieren und deaktivieren sowie Änderungen durchführen.

Um den Regel-Assistenten zu schließen klicken Sie auf die Schaltfläche **OK**.

5.5.7. Proxy Content Manager


Proxy Content
Entries per page: 10
Show type: All
40 items, 40 shown
Pages: 1 | 2 | 3 | 4
A
ID
Type
Date / Time
2003-01-28-07-01-14-8340-1
pop3
2003-01-28 07:28
This message was intercepted by the POP3 proxy. It contains a virus or other harmful content.
2003-01-28-07-01-47-3095-2
pop3
2003-01-28 07:24
This message was intercepted by the POP3 proxy. It contains a virus or other harmful content.
1BafzY-00011z-00
smtp_err
2003-01-20 18:45
[bounce] -> do-not-reply@fw-notify.net
Subject: [mx.domain.example] [WAR 035] Mail delivery failed : returning message to sender
Content Scanner: [no checks done]
Cause: 2003-01-20 18:45:48 do-not-reply@fw-notify.net R=dnslookup T=remote_smtp: retry time not reached for any host after a long failure period
*** Frozen (delivery error message)
1Bafym-0000OG-00
smtp_err
2003-01-20 18:41
[bounce] -> do-not-reply@fw-notify.net
Subject: [mx.domain.example] [WAR 035] Mail delivery failed : returning message to sender
Content Scanner: [no checks done]
Cause: 2003-01-20 18:41:54 do-not-reply@fw-notify.net R=dnslookup T=remote_smtp: retry time not reached for any host after a long failure period
*** Frozen (delivery error message)
2003-01-20-07-01-09-14025-2
pop3
2003-01-20 07:52
This message was intercepted by the POP3 proxy. It contains a virus or other harmful content.
1BaCgb-00061r-00
smtp_err
2003-01-19 11:28
[bounce] -> do-not-reply@fw-notify.net
Subject: [mx.domain.example] [WAR 035] Mail delivery failed : returning message to sender
Content Scanner: [no checks done]

Im Menü **Proxy Content Manager** können Sie alle E-Mails einsehen, die von den Proxies der Firewall gefiltert wurden oder wegen eines Fehlers nicht weitergeleitet werden konnten.

Die nachfolgend aufgeführten Begriffe und Stati benötigen Sie, um die E-Mails in diesem Menü korrekt zu verwalten:

ID: Jede E-Mail in diesem Internet-Sicherheitssystem erhält eine eindeutige **ID**. Diese **ID** ist im Header einer Mail enthalten und identifiziert außerdem die E-Mail in den Log Files.

Type: Der Proxy Content Manager unterteilt die gefilterten E-Mails in drei Typen:

- **smtp_queue**: Die E-Mail wird an die Empfängeradresse versendet. Falls eine E-Mail mit diesem Status längere Zeit auf der Firewall liegen bleibt, so deutet dies auf temporäre Probleme auf dem Zielhost hin. Die E-Mail wird ausgeliefert, sobald der Zielhost wieder in der Lage ist, sie anzunehmen.
- **smtp_err**: Die E-Mail wurde entweder als **Frozen bounce** eingestuft oder aufgrund der Einstellung **Quarantine** in einer der SMTP-Content-Control-Module in Quarantäne genommen. In der E-Mail wurden unerwünschte oder für Ihr System sogar gefährliche Komponenten, z. B. Viren entdeckt. E-Mails mit diesem Status werden niemals versendet, es sei denn, dass dies explizit beabsichtigt wird. E-Mails mit diesem Status

verbleiben in der Tabelle bis sie von Ihnen gelöscht oder explizit versendet werden.

- **pop3**: Die E-Mail wurde wegen Verdacht auf einen Virus vom POP3-Proxy gefiltert.

E-Mails mit dem Typ **smtp_err** können folgende Stati erhalten:

Bounce: Die E-Mail konnte nicht an die Empfängeradresse gesendet werden. Dieser Status wird auch generiert falls die E-Mail an mehrere Empfängeradressen abgeschickt wurde, aber nur ein Teil der Empfänger diese E-Mail auch tatsächlich erhalten hat. Der Absender wird über diesen Status benachrichtigt, indem die E-Mail an ihn mit einer entsprechenden Nachricht zurückgesendet wird.

Frozen: Beim Versuch die E-Mail zu versenden, wurde ein permanenter Fehler verursacht. Dies geschieht normalerweise, wenn der Status **Bounce** nicht an die original Absenderadresse geschickt werden kann.

Frozen bounce: Dieser Status ist eine Kombination aus den zwei zuvor beschriebenen Stati.

Der Content Manager

Entries per Page: Mit diesem Drop-down-Menü stellen Sie ein, wie viele Einträge pro Seite angezeigt werden. Per Default ist **10** Einträge pro Seite eingestellt.

Show type: Hier stellen Sie ein welcher Typ angezeigt werden soll. Per Default ist **All** eingestellt.

Auf der rechten Seite wird die Gesamtsumme der E-Mails im Proxy Content Manager angezeigt. Die Angabe rechts daneben ergibt sich aus der Einstellung mit dem Drop-down-Menü **Show type**.

Für jede gefilterte E-Mail wird in dieser Tabelle eine Zeile erzeugt. Durch einen Klick auf die Mail-**ID** in der Spalte **ID** können Sie die E-Mail öffnen und wichtige Nachrichten gefahrlos lesen. Falls verfügbar, steht unter der **ID** die Absenderadresse und der erste Empfänger. Falls keine Absenderadresse vorhanden ist, wird hier `[bounce]` angezeigt. E-Mails mit dem Status **Frozen** und/oder **Bounce** werden nach sieben Tagen aus der Tabelle gelöscht.

In der Zeile **Subject** wird der Hostname und eine Notification mit Informations-Code angezeigt. Die Fehler-, Warnungs- und Informations-Codes sind im Kapitel 5.8.11 ab Seite 248 aufgeführt.

In der Zeile **Content Scanner** werden Informationen angezeigt, wenn die E-Mail aufgrund eines Content-Control-Checks gefiltert wurde. Die Meldung enthält in diesem Fall den Namen des Viruses oder die Spambewertung. Falls die Nachricht nicht wegen eines Content-Control-Checks gefiltert wurde erscheint die Meldung **no checks done**.

Unter **Cause** sind neben Datum und Uhrzeit des E-Mails weitere Informationen enthalten, um die gefilterte Nachricht zu bewerten.

Im Drop-down-Menü am unteren Ende der Tabelle befinden sich mehrere Funktionen, um einzelne E-Mails zu bearbeiten. Die E-Mails müssen zuvor durch einen Klick auf das entsprechende Optionsfeld ausgewählt werden.
Folgenden Funktionen stehen zur Verfügung:

Delete: Alle ausgewählten E-Mails werden gelöscht.

Forward to postmaster: Die E-Mails werden an den **Postmaster** weitergeleitet. Die E-Mail-Adresse des Postmasters definieren Sie im Menü **Proxies/SMTP**.

SMTP: Cancel message: Die E-Mails werden mit dem Vermerk **cancelled by administrator** an die jeweiligen Absender zurückgeschickt. Diese Funktion kann nur am Typ **smtp_queue** angewendet werden.

SMTP: Attempt dequeue: Der Status der E-Mail wird zurückgesetzt und der Versuch wird gestartet diese sofort zu versenden. Falls durch diese E-Mail nochmals ein Fehler verursacht wird, erhält Sie wieder den alten Status. Diese Funktion ist bei den Typen **smtp_queue** und **smtp_err** möglich.

Delete all Content of Type

Um den belegten Festplattenspeicher Ihres Internet-Sicherheitssystems möglichst gering zu halten, können Sie hier alle E-Mails eines bestimmten Typs löschen.
E-Mails, die während des Löschvorgangs vom Internet-Sicherheitssystem versendet oder weitergeleitet werden, sind davon nicht betroffen.

Achtung:

Der ausgewählte Typ wird ohne eine nochmalige Sicherheitsabfrage gelöscht.

5.6. Virtual Private Networks (IPSec VPN)

Ein **Virtuell Private Network (VPN)** ist eine sichere Kommunikationsverbindung über ein ungesichertes Netzwerk, z. B. das Internet.
Ein **VPN** ist immer dann nützlich, wenn Informationen über das Internet gesendet oder empfangen werden und gewährleistet sein muss, dass diese Informationen von keinem Dritten gelesen oder verändert werden können. Diese Verbindung wird durch die Software gesichert, die auf beiden Seiten der Verbindung installiert ist. Diese Software ermöglicht Authentifizierung, Schlüsselaustausch und Datenverschlüsselung nach dem offenen Standard **Internet Protocol Security (IPSec)**.

Bei einer durch **VPN** geschützten Verbindung können nur authentifizierte Gegenstellen miteinander kommunizieren. Niemand anderes kann Informationen über diese Verbindung übertragen, lesen oder verändern.
Eine VPN-Verbindung kann entweder zwei Hosts, einen Host und ein Netzwerk (LAN) oder zwei Netzwerke gesichert miteinander verbinden. Wenn an einem VPN-Endpunkt ein Host angeschlossen ist, so reicht der VPN-Tunnel bis zu diesem Rechner und wird dort ver- und entschlüsselt. Bei einem Netzwerk ist ein **Security Gateway** vorhanden, welches die VPN-Verbindung verwaltet und die Daten ver- und entschlüsselt. Der Datenverkehr zwischen dem Security Gateway und dem Netzwerk ist nicht verschlüsselt.
Der Datenaustausch zwischen zwei Gegenstellen über das **Public Wide Area Network (WAN)** erfolgt über öffentliche Router, Switches und andere Netzwerkkomponenten und wird allgemein als unsicher angesehen. Es besteht theoretisch an jedem dieser Punkte die Möglichkeit gesendete Nachrichten im Klartext mitzulesen. Mit Hilfe von **IPSec VPN** wird zwischen den beiden Endpunkten ein virtueller verschlüsselter **IP Security (IPSec)**-Tunnel durch das **WAN** erzeugt.

Ein **IPSec**-Tunnel besteht aus einem Paar richtungsgebundener **Security Associations (SA),** einem für jede Richtung der Kommunikation.

Ein **IPSec SA** besteht aus drei Komponenten:

dem **Security Parameter Index (SPI)**,

der IP-Adresse des Empfängers

einem **Security Protocol** - **Authentication Header (AH)** oder **Encapsulation Security Payload (ESP)**.

Die **SA** ermöglicht dem **IPSec VPN**-Tunnel folgende Sicherheitsfunktionen:

Geheimhaltung durch Verschlüsselung

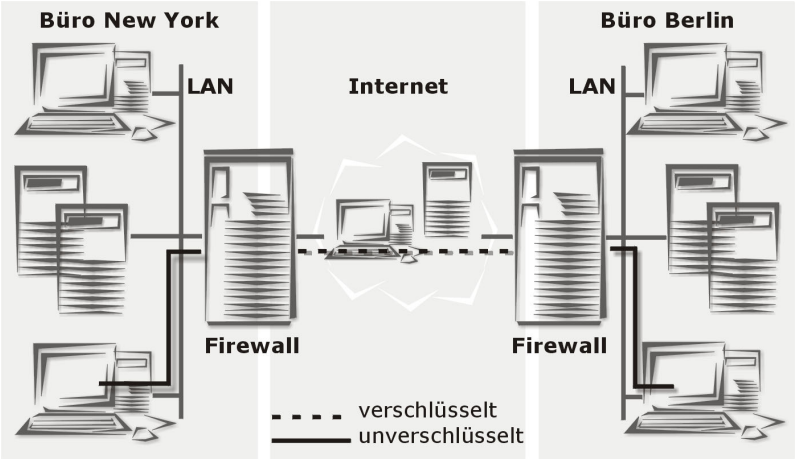
Datenintegrität durch Datenauthentifizierung

Senderauthentifizierung durch PSK, RSA oder X.509-Zertifikate

Die Sicherheitsfunktionen können beliebig kombiniert werden und richten sich nach den aktuellen Anforderungen. Die meisten Netzwerksicherheits-Designer verwenden die Verschlüsselung und die Authentifizierung.

Es gibt mehre Szenarien eine VPN zu nutzen:

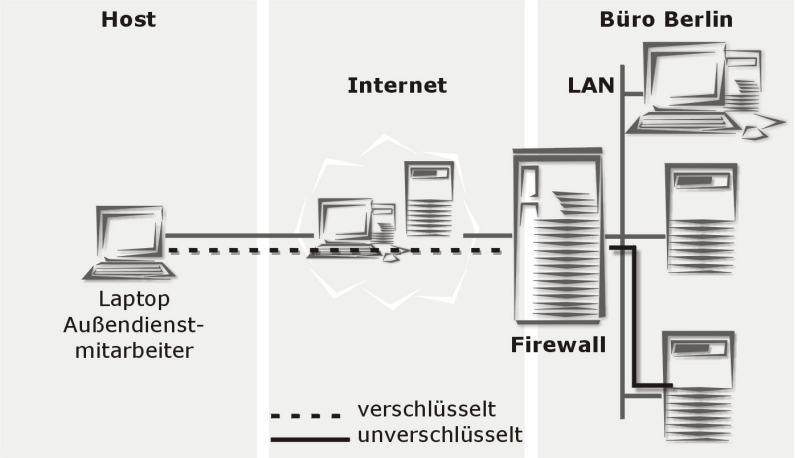
1. NET to NET-Verbindung



Ein Netzwerk kommuniziert mit einem anderen Netzwerk.
Zwei Unternehmens-Netzwerke von örtlich getrennten Niederlassungen können VPN nutzen, um miteinander zu kommunizieren, als wären sie ein Netzwerk.

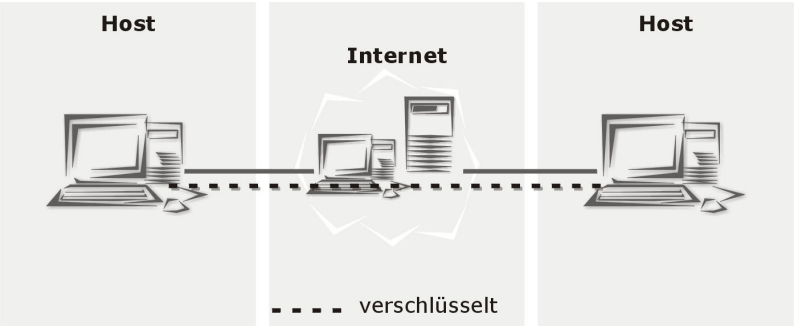
Diese Art der Verbindung könnte man auch nutzen, um vertrauenswürdigen Firmen (Zulieferer, Berater) gesicherten Zugriff auf interne Informationen zu ermöglichen.

2. HOST to NET-Verbindung



Ein Computer kommuniziert mit einem Netzwerk.
Außendienstmitarbeiter oder Heimarbeiter können VPN benutzen, um sicher mit dem Unternehmens-Netzwerk zu kommunizieren.

3. HOST to HOST-Verbindung



Ein Computer kommuniziert mit einem anderen Computer.
Zwei Computer können durch VPN über das Internet kommunizieren, um ihren Informationsaustausch zu verschlüsseln.

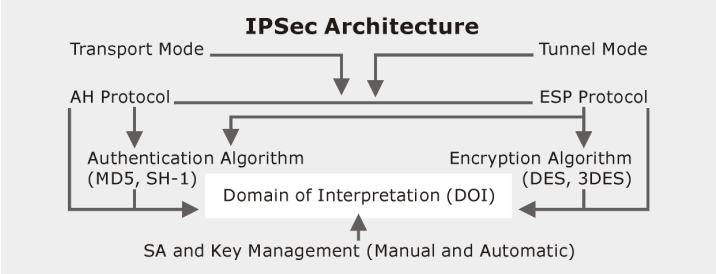
Ein VPN-Server ist eine kostengünstige und sichere Lösung um Informationen zu übertragen und kann teuere Datendirekt-Verbindungen (Standleitungen) zwischen Unternehmen ersetzen.

Das IPSec-Konzept

IP Security (IPSec) ist eine Suite von verschiedenen Protokollen für die kryptographische, sichere Kommunikation auf IP-Ebene/ Layer 3 (siehe auch Kapitel 2, ab Seite 10).
IPSec besteht aus zwei Betriebsarten (Modi) und aus zwei Protokollen:

- **Transport-Modus**
- **Tunnel-Modus**
- **Authentication Header (AH)** Protokoll für Authentifizierung
- **Encapsulation Security Payload (ESP)** Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet **IPSec** Methoden für die manuelle sowie die automatische Verwaltung von **Security Associations (SA)** und zur Schlüsselverteilung. Alle diese Merkmale wurden in einem **Domain of Interpretation (DOI)** zusammengefasst.

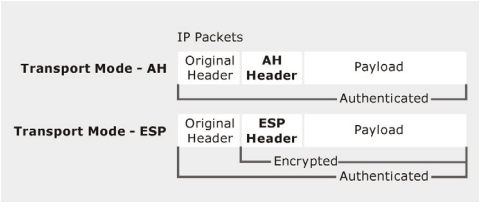


Hinweis:

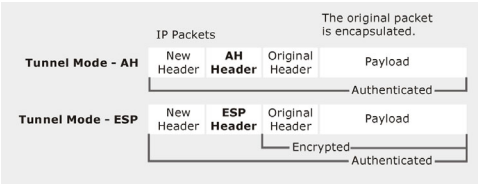
Das Internet-Sicherheitssystem unterstützt den **Tunnel Mode** und das **Encapsulation Security Payload (ESP)** Protokoll.

IPSec Modi

IPSec arbeitet im **Transport-Modus** oder **Tunnel-Modus**. Bei einer Host to Host-Verbindung kann grundsätzlich entweder Transport oder Tunnel Modus verwendet werden. Falls einer der beiden Tunnelendpunkte ein Security Gateway ist, muss der Tunnel Modus verwendet werden. Die IPSec VPN-Verbindungen dieses Internet-Sicherheitssystems arbeiten immer im Tunnel-Modus.



Beim **Transport-Modus** wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird nach einem entsprechenden Protokoll Header als Payload entweder im Klartext **(AH)** oder verschlüsselt **(ESP)** angehängt. Nun kann entweder das komplette Paket mit **AH** authentifiziert oder die Payload mit Hilfe von **ESP** verschlüsselt werden.
Bei beiden Varianten wird der original Header in Klartext über das WAN geschickt.



Beim **Tunnel-Modus** wird das komplette Paket – Header und Payload – in ein neues IP-Paket als Payload eingepackt. Ein neuer IP-Header wird vorne an das IP-Paket angehängt. Die IP-Adressen des neuen Header entsprechen denen der IPSec-Tunnelendpunkte. Die IP-Adressen des eingepackten Paketes bleiben unverändert. Das komplette Originalpaket kann nun verschlüsselt und/oder authentifiziert werden. Mit **AH** kann das komplette Paket authentifiziert werden. Mit dem Verschlüsselungs-Protokoll **ESP** ist dies lediglich ab dem ESP-Header möglich.

IPSec-Protokolle

IPSec verwendet für die sichere Kommunikation auf der IP-Ebene zwei Protokolle.

- **Authentication Header (AH)** – ein Sicherheitsprotokoll für die Authentifizierung des Absenders sowie zur Überprüfung der Integrität des Inhalts
- **Encapsulating Security Payload (ESP)** – ein Sicherheitsprotokoll für die Verschlüsselung des kompletten Paketes (sowie für die Authentifizierung des Inhalts)

Das **Authentication Header**-Protokoll **(AH)** ermöglicht die Überprüfung der Authentizität und der Integrität des Paketinhalts. Des Weiteren wird geprüft, ob die Sender- und Empfänger-IP-Adresse geändert wurde. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines Hash-based Message Authentication Codes (HMAC) in Verbindung eines Schlüssels und einem der folgenden Hash-Algorithmen berechnet wurde:

Der **Message Digest Version 5 (MD5)-**Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge einen 128 bit langen Hash-Wert. Dieser resultierende Hash-Wert wird als eine Art Fingerabdruck des Paketinhalts verwendet, um den Absender zu prüfen. Dieser Hash-Wert wird auch als **digitale Signatur** oder als **Message Digest** bezeichnet.
Der **Secure Hash (SHA-1)**-Algorithmus erzeugt analog zum **MD5** einen 160 bit langen Hash-Wert. **SHA-1** ist aufgrund des längeren Schlüssels sicherer als **MD5**.
Der Aufwand einen Hash-Wert mittels **SHA-1** zu berechnen ist im Vergleich zum **MD5**-Algorithmus etwas höher. Dies kommt allerdings infolge der heutigen Prozessor-Performance nur zum tragen, wenn sehr viele **IPSec VPN**-Verbindungen über ein **Security Gateway** verschlüsselt werden.

Das **Encapsulation Security Payload**-Protokoll **(ESP)** bietet zusätzlich zur Verschlüsselung auch die Möglichkeit der Absender –Authentifizierung und der Inhaltsverifizierung. Wenn man **ESP** im **Tunnel-Modus** verwendet, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt. Der neue IP-Header beinhaltet Absender- und

Empfänger-IP-Adresse. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

ESP mit Verschlüsselung ist grundsätzlich mit folgenden Verschlüsselungs-Algorithmen möglich:

- Keine Verschlüsselung (NULL)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Eine hohe Sicherheit erreicht man durch Verwenden von AES. Die effektiven Schlüssellängen von AES sind wahlweise 128, 192 oder 256 Bits. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt mehrere Verschlüsselungs-Algorithmen.

Für die Authentifizierung kann wieder der MD5- oder der SHA-1-Algorithmus verwendet werden.

Schlüsselverwaltung (Key Management)

Die sichere Erzeugung, Verwaltung und Verteilung der Schlüssel ist ausschlaggebend für die erfolgreiche Nutzung einer VPN-Verbindung. IPSec unterstützt die manuelle (Manual Keying) sowie die automatische Schlüsselverteilung (Internet Key Exchange).

Für die **manuelle Schlüsselverteilung (Manual Keying)** müssen beide Seiten des VPN-Tunnels von Hand konfiguriert werden. Im Detail bedeutet dies, dass für jede der beiden **Security Associations (SA)** – immer zwei je VPN-Tunnel – ein **Security Parameter Index (SPI)** ausgewählt, je ein Schlüssel für die Verschlüsselung und die Authentifizierung generiert werden muss und diese Schlüssel auf beiden Seiten installiert werden müssen. Diese Schlüssel sollten später in regelmäßigen Abständen gegen neue ersetzt werden.
Die manuelle Schlüsselverteilung ist sehr aufwendig. Des Weiteren birgt dieses Verfahren einige Sicherheitsrisiken, da gewährleistet sein muss, dass Unbefugte keinen Zugang zu den Schlüsseln haben.
Bei neuen Installationen wird **Manual Keying** heute nur noch selten verwendet.

Mit Hilfe des **Internet Key Exchange (IKE)**-Protokolls führt **IPSec** die Schlüsselverwaltung selbständig durch. Die Schlüssel werden automatisch erzeugt und sicher ausgetauscht. Das **IKE**-Protokoll ermöglicht das Erzeugen und Verwalten mehrerer VPN-

Tunnel sowie die Verwendung von dynamischen IP-Adressen. Außerdem werden vom **IKE**-Protokoll die **Security Associations (SA)** automatisch verwaltet.

Das Internet-Sicherheitssystem unterstützt drei Authentifizierungsarten innerhalb des IKE-Protokolls:

- IKE mit Preshared Keys (PSK)
- IKE mit RSA Keys (RSA)
- IKE mit X.509v3-Zertifikaten (X509)

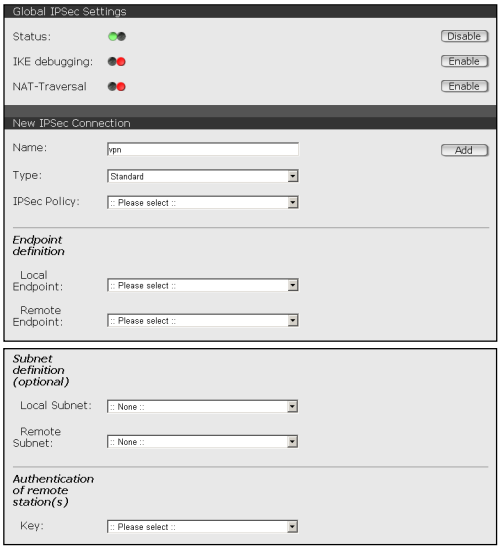
Die Authentifizierung mit **Preshared Keys (PSK)** erfolgt durch Schlüssel mit einem geheimen Kennwort, die vor der eigentlichen Verbindung unter den Beteiligten ausgetauscht werden. Wenn nun ein VPN-Tunnel aufgebaut werden soll, prüfen die beiden Gegenstellen, ob ihnen dieses geheime Kennwort bekannt ist. Wie sicher solche **PSK**s sind, hängt davon ab, wie „gut" das Kennwort gesetzt wurde. Allgemeine Wörter sind z. B. sehr unsicher, da sie sehr anfällig auf Wörterbuch-Angriffe sind. Daher sollte bei dauerhaften IPSec VPN-Verbindungen diese Authentifizierungsmethode durch Zertifikate oder durch RSA ersetzt werden.

Die Authentifizierung mit **RSA Keys** basiert auf einem Schlüssel-(Key)-Paar und beinhaltet einen **Public Key** (öffentlichen Schlüssel) und einen **Private Key** (privaten Schlüssel). Der **Private Key** wird zur Verschlüsselung und Authentifizierung während des **Key Exchanges** (Schlüsselaustausch) benötigt. Die beiden Schlüssel sind mathematisch voneinander abhängig und stehen in einer einzigartigen Verbindung zueinander: Daten, die mit einem Schlüssel verschlüsselt wurden, können nur mit dem anderen Schlüssel wieder entschlüsselt werden. Der **Private Key** kann nicht vom **Public Key** abgeleitet werden.
Beide Gegenstellen einer IPSec VPN-Verbindung benötigen bei dieser Authentifizierungsmethode ihren eigenen **Public Key** und **Private Key**.

Das **X.509-Zertifikat** basiert ähnlich wie die Authentifizierung mit RSA Keys auf den Schlüsselpaaren **Public Key** und **Private Key**. Ein X.509-Zertifikat entspricht dem **Public Key** mit zusätzlichen spezifischen Informationen. Dieses Zertifikat wird wird durch eine **Certificate Authority (CA)** Ihres Vetrauens signiert. Während des **Key Exchange** werden die Zertifikate ausgetauscht und durch das lokal gespeicherten CA-Zertifikat überprüft.

Weitere Informationen zu **Certificate Authority (CA)** erhalten Sie in Kapitel 5.1.7 ab Seite 86 und in Kapitel 5.6.5 ab Seite 232.

5.6.1. Connections



Im Menü **Connections** definieren Sie die lokalen Einstellungen für einen neuen **IPSec**-Tunnel oder editieren und beobachten die bestehenden Verbindungen.

Global IPSec Settings

In diesem Fenster schalten Sie **IPSec VPN** durch einen Klick auf die Schaltfläche **Enable**/**Disable** neben **Status** ein und aus.

IKE Debugging: Diese Funktion steht Ihnen zur Überprüfung der IPSec-Verbindung zur Verfügung. Mit dieser Funktion werden in den IPSec-Logs ausführliche Informationen protokolliert. Diese Protokolle können Sie mit der Funktion **Live Log** entweder weiter unten im Fenster **IPSec Live Log** oder im Menü **Log Files/ IPSec VPN** in Echtzeit beobachten oder auf Ihren lokalen Rechner herunterladen. Die Funktionen im Menü **Log Files** werden im Kapitel 5.8 ab Seite 244 beschrieben.

Wichtiger Hinweis:

Die Funktion **IKE Debugging** benötigt einen großen Teil der Systemresourcen und kann daher den IPSec VPN-Verbindungsaufbau erheblich verlangsamen. Schalten Sie daher die Funktion nur für den eigentlichen Debugging-Vorgang ein.

NAT Traversal: Wenn diese Funktion eingeschaltet ist, können Hosts einen IPSec-Tunnel durch NAT-Geräte aufbauen. Dieses Modul versucht zu ermitteln, ob zwischen Server und Client NAT-

Geräte verwendet werden. Wenn NAT-Geräte entdeckt werden, verwendet das System zur Kommunikation mit dem externen Host UDP-Pakete. Dies funktioniert allerdings nur, wenn beide IPSec-Endpunkte NAT Traversal unterstützen und auf dem Road-warrior-Endpunkt eine virtuelle IP-Adresse eingestellt ist.
Zusätzlich muss auf dem NAT-Gerät der IPSec-Durchgang ausgeschaltet sein, da dies NAT Traversal unterbrechen kann.

Wichtiger Hinweis:

Für die Funktion **Virtual IP** können keine lokalen IP-Adressen verwendet werden, da das Internet-Sicherheitssystem keine ARP-Anfragen für diese Adressen beantwortet.

IPSec Connections

In der Tabelle **IPSec Connections** werden alle aktuellen VPN-Verbindungen angezeigt.

VPN Status

Im Fenster **VPN Status** wird der Status der aktiven Verschlüsselungs-Algorithmen, alle aktiven IPSec-Verbindungen und detaillierte Informationen zu jeder **Security Association (SA)** angezeigt.

VPN Routes

Im Fenster **VPN Routes** werden alle aktiven IPSec-SA-Verbindungen angezeigt. Solange hier keine Einträge vorhanden sind, existieren keine IPSec-Verbindungen.

Routing-Einträge werden nach folgendem Schema angezeigt:

```
A B                  -> C                  => D

3 192.168.105.0/24 -> 192.168.104.0/24 => %hold

8 192.168.105.0/24 -> 192.168.110.0/24 => %trap

0 192.168.105.0/24 -> 192.168.130.0/24 =>
                      tun0x133a@233.23.43.1
```

Spalte **A**: Anzahl der Pakete in dieser VPN-Verbindung.

Spalte **B**: Das lokale Sub-Netzwerk oder den Host.

Spalte **C**: Das entfernte Sub-Netzwerk oder den Host.

Spalte **D**: Der Status der VPN-Verbindung.

%trap: Die Verbindung ist im Leerlauf und wartet bis ein Datenpaket eintrifft. Dieser Status leitet die Aushandlung der VPN-Verbindung ein.

%hold: Die Aushandlung dauert an. Das bedeutet, dass alle Datenpakete gehalten werden bis der VPN-Tunnel hochgefahren (UP) ist.

tun0x133a@233.23.43.1: Diese oder eine ähnliche Meldung wird angezeigt, sobald der Tunnel hochgefahren ist:
Ein VPN-Tunnel mit der ID `0x133a` ist hochgefahren und die IP-Adresse des **Remote Endpoint** ist `233.23.43.1`..

Beispiel:

```
A B                   -> C                  => D

23 192.168.105.0/24 -> 192.168.104.0/24 =>
                       tun0x1234@123.4.5.6
```

In diesem VPN-Tunnel wurden 23 Datenpakete vom Netzwerk `192.168.105.0/24` zum Netzwerk `192.168.104.0/24` geschickt. Der Tunnel hat die ID `0x1234` und der Remote Endpunkt hat die IP-Adresse `123.4.5.6`..

IPSec Live Log

Das heutige Protokoll kann durch einen Klick auf die Schaltfläche **View IPSec Live Log** geöffnet und in Echtzeit beobachtet werden. Diese Funktion steht auch im Menü **Log Files/IPSec VPN** zur Verfügung.

IPSec-Verbindung konfigurieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Connections**.

2. Schalten Sie im Fenster **Global IPSec Settings** das Modul durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich das Fenster **New IPSec Connection**.

3. Tragen Sie im Eingabefeld **Name** einen Namen für die neue IPSec VPN-Verbindung ein:

   Name: Definieren Sie einen Namen, der diesen IPSec VPN-Tunnel eindeutig beschreibt.
   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

   Type: Wählen Sie hier den Verbindungs-Typ aus.

   Der Typ **Standard** dient für **NET to NET**-Verbindungen.

   Der Typ **Roadwarrior** eignet sich für **HOST to NET**-Verbindungen, z. B. für Außendienstmitarbeiter. Diese können über ihr Laptop eine IPSec-Verbindung zum firmeninternen LAN aufbauen. Eine Roadwarrior-Verbindung kann nur über ein **Default Gateway** angeschlossen werden.

   Hinweis:
   An eine Roadwarrior-Verbindung können mehrere Remote-Key-Objekte hinzugefügt werden. Der Konfigurationsaufwand wird dadurch erheblich verringert.

   Die weiteren Einstellungen richten sich nun nach dem ausgewählten Verbindungs-Typ.

4. Wählen Sie im Drop-down-Menü **IPSec Policy** eine Policy aus.

   In der Policy werden die Parameter für die IPSec-Verbindung generiert. Dies beinhaltet die Einstellung der **Key Exchange-**Methode **IKE** und der **IPSec**-Verbindung.

   Im Drop-down-Menü sind bereits vordefinierte Policies enthalten. Im Menü **IPSec VPN/Policies** können Sie eigene **IPSec Policies** konfigurieren.

Die Konfiguration einer **IPSec Policy** wird in Kapitel 5.6.2 ab Seite 223 beschrieben.

5. Wählen Sie im Fenster **Endpoint Definition** die Endpunkte des IPSec-Tunnels aus.

   Local Endpoint: Wählen Sie hier den lokalen Endpunkt aus. Wählen Sie als lokalen Endpunkt immer die Netzwerkkarte aus, die in Richtung des anderen Endpunktes zeigt.

   Remote Endpoint: Wählen Sie hier die IP-Adresse des entfernten Endpunktes aus.
   Bei einer Roadwarrior-Verbindung hat der entfernte Endpunkt immer eine dynamische IP-Adresse.

6. Im Fenster **Subnet Definition (optional)** können Sie für beide Endpunkte optional ein Sub-Netzwerk auswählen.
   Wenn Sie eine Roadwarrior-Verbindung erstellen, kann für **Remote Subnet** kein Netzwerk definiert werden.

   Local Subnet: Wählen Sie hier das lokale Sub-Netzwerk aus.

   Remote Subnet: Wählen Sie hier das entfernte Sub-Netzwerk aus.

7. Wählen Sie nun im Fenster **Authentication of Remote Station(s)** den passenden **Key** aus.
   Die IPSec-Remote-Keys werden im Menü **IPSec VPN/Remote Key** definiert. Für jeden entfernten Endpunkt wird ein IPSec-Remote-Key-Objekt benötigt.

8. Speichern Sie nun die Einstellungen durch einen Klick auf die Schaltfläche **Add**.

Das neu konfigurierte IPSec-Verbindungsprofil wird immer deaktiviert an letzter Stelle in die Tabelle eingetragen (Statusampel zeigt Rot). Durch einen Klick auf die Statusampel wird die IPSec-Verbindung aktiviert.

Nachdem Sie einen VPN-Tunnel erstellt haben, müssen Sie noch die entsprechenden Paketfilterregeln setzen, die es den jeweiligen Parteien erlauben, miteinander zu kommunizieren.
Das Setzen von Paketfilterregeln wird in Kapitel 5.4 ab Seite 164 beschrieben.

Beispiel:

Wenn Sie eine Net to Net-VPN-Verbindung (zwischen Netzwerk 1 und Netzwerk 2) erstellt haben und die komplette Kommunikation zwischen diesen beiden Netzwerken erlauben möchten, müssen Sie die folgenden zwei Regeln setzen:

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules**.
2. Setzen Sie im Fenster **Add Rules** die folgende Regel für das Netzwerk 1:

   From (Client): Netzwerk1

   Service: Any

   To (Server): Netzwerk2

   Action: Allow
3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.
4. Setzen Sie im Fenster **Add Rules** die folgende Regel für das Netzwerk 2:

   From (Client): Netzwerk2

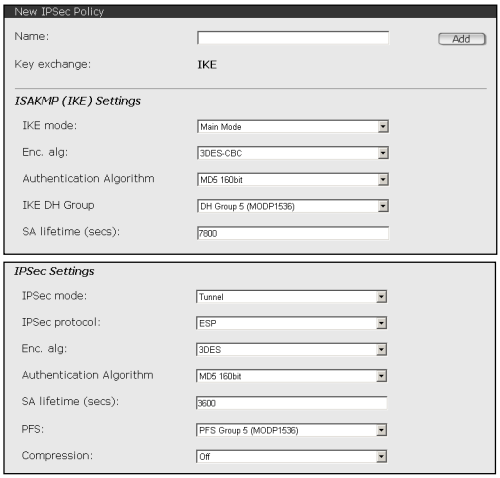
   Service: Any

   To (Server): Netzwerk1

   Action: Allow
5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Anschließend ist die komplette Kommunikation zwischen den beiden VPN-Gegenstellen möglich.

5.6.2. Policies



Im Menü **Policies** definieren Sie die Parameter für die IPSec -Verbindung und generieren daraus eine Policy. Die Policy wird für die Erstellung einer IPSec-Verbindung benötigt und beinhaltet die Konfiguration der **Key Exchange**-Methode **IKE** und die der **IPSec**-Verbindung.

Der **Key Exchange** steht für die Art des Schlüsselaustausches der IPSec-Verbindung.

Die gängigen Varianten sind:

Manual Key Exchange
Internet Key Exchange (IKE)

Das IPSec VPN dieses Internet-Sicherheitssystems unterstützt IKE als Key-Exchange-Methode. Die Manual-Key-Exchange-Methode ist nicht möglich.

IPSec Policy konfigurieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Policies**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **New IPSec Policy** zu öffnen.
3. Tragen Sie im Eingabefeld **Name** einen Namen für die neue IPSec Policy ein:

   Name: Definieren Sie einen Namen, der diese Policy eindeutig beschreibt, z. B. den verwendeten Verschlüsselungs-Algorithmus. Sie können den Namen auch im letzten Schritt vor dem Erzeugen der Policy definieren.

   Key exchange: Als Schlüsselaustauschs-Methode wird nur **IKE** unterstützt.

4. Definieren Sie im Fenster **ISAKMP (IKE) Settings** die Einstellungen für die IKE-Verbindung:

   IKE mode: Der IKE-Modus beschreibt das für den Schlüsselaustausch nötige Protokoll. Derzeit wird nur **Main Mode** unterstützt.

   Encryption algorithm: Der Encryption Algorithmus beschreibt den Algorithmus für die Verschlüsselung der IKE-Verbindung. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **3DES-CBC**, **Blowfish**, **Rijndael (AES) 128bit keylength**, **Rijndael (AES) 192bit keylength**, **Rijndael (AES) 256bit keylength**, **Serpent 128bit keylength** und **Twofish**.

   Authentication algorithm: Hier wird angezeigt, welcher Algorithmus verwendet wird, um die Vollständigkeit der IKE-Nachricht zu prüfen. Unterstützt werden die Algorithmen **MD5 128bit**, **SHA1 160bit**, **SHA2 256bit** und **SHA2 512bit**. Der zu verwendende Algorithmus wird von der Gegenstelle der IPSec-Verbindung bestimmt.

   Wichtiger Hinweis:

   Die Algorithmen **SHA2 256bit** und **SHA2 512bit** benötigen einen hohen Anteil der Systemresourcen.

   IKE DH Group: Die IKE Group (Diffie-Hellmann Group) bezeichnet und beschreibt die asymetrische Verschlüsselung während des Schlüsselaustauschs. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X (MODP 3072)** und **Group X (MODP 4096)**. Die zu verwendende Gruppe wird von der Gegenstelle der IPSec-Verbindung bestimmt.

   SA lifetime (secs): Hier definieren Sie die Dauer der IKE-Verbindung in Sekunden. Nach der Installation sind standardmäßig 7800 Sekunden (2h, 10 min) eingestellt.
   Generell ist eine Zeitspanne zwischen 60 und 28800 Sekunden (8 Stunden) möglich.

5. Definieren Sie im Fenster **IPSec Settings** die Einstellungen für die IPSec-Verbindung:

   IPSec mode: Dieses System unterstützt nur den **Tunnel Mode**.

IPSec protocol: Dieses System unterstützt nur das Protokoll **ESP**.

Encryption algorithm: Hier wählen Sie den Algorithmus für die Verschlüsselung der IPSec-Verbindung aus.
Dieses System unterstützt die Verschlüsselungs-Algorithmen **3DES**, **Blowfish**, **Rijndael (AES) 128bit keylength**, **Rijndael (AES) 192bit keylength**, **Rijndael (AES) 256bit keylength** und **Twofish**. Wenn Sie die IPSec-Verbindung ohne Verschlüsselung aufbauen möchten wählen Sie **null** aus.

Enforce algorithm: Wenn ein IPSec Gateway einen Vorschlag bzgl. eines Verschlüsselungsalgorithmus und der Stärke macht, kann es vorkommen, dass das Gateway der Gegenstelle diesen Vorschlag annimmt, obwohl die IPSec Policy diesem nicht entspricht. Um dies zu verhindern, muss **Enforce algorithm** aktiviert werden.

Beispiel:

Die IPSec Policy fordert AES-256 als Verschlüsselung. Ein Roadwarrior mit **SSH Sentinel** will aber mit AES-128 verbinden. Ohne **Enforce algorithm** wird die Verbindung trotzdem zugelassen, was ein Sicherheitsrisiko darstellt.

Authentication algorithm: Unterstützt werden die Algorithmen **MD5 128bit**, **SHA1 160bit**, **SHA2 256bit** und **SHA2 512bit**. Der zu verwendende Algorithmus wird von der Gegenstelle der IPSec-Verbindung bestimmt.

Wichtiger Hinweis:

Die Algorithmen **SHA2 256bit** und **SHA2 512bit** benötigen einen hohen Anteil der Systemresourcen.

SA lifetime (secs): Hier definieren Sie die Dauer der IPSec-Verbindung in Sekunden. Nach der Installation sind standardmäßig 3600 Sekunden (1h) eingestellt.
Generell ist eine Zeitspanne zwischen 60 und 28800 Sekunden möglich.

PFS: Die IPSec-Schlüssel für die IPSec-Verbindung werden auf der Basis von Zufallsdaten generiert. Mit **Perfect Forwarding Secrecy (PFS)** wird sichergestellt, dass diese Zufallsdaten nicht bereits zur Erstellung eines anderen Schlüssels, z. B. für die IKE-Verbindung, verwendet wurden.

Falls ein älterer Schlüssel gefunden oder berechnet wird, können daher keinerlei Rückschlüsse auf den neuen Schlüssel gezogen werden.
Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X (MODP 3072)** und **Group X (MODP 4096)**. Wenn Sie **PFS** ausschalten möchten wählen Sie **No PFS** aus.

Per Default ist bei dieser Funktion bereits **Group 5 (MODP 1536)** eingestellt.

Wichtiger Hinweis:

PFS benötigt durch den **Diffie-Hellmann**-Schlüsselaustausch zusätzliche Rechenleistung. **PFS** ist außerdem nicht immer 100%-ig kompatibel unter den verschiedenen Herstellern. Bei Problemen mit der Rechner-Performance oder mit dem Verbindungsaufbau zur Gegenstelle schalten Sie diese Funktion bitte aus.

Compression: Mit Hilfe dieser Algorithmen können Sie die IP-Pakete, bevor sie verschlüsselt werden, komprimieren.

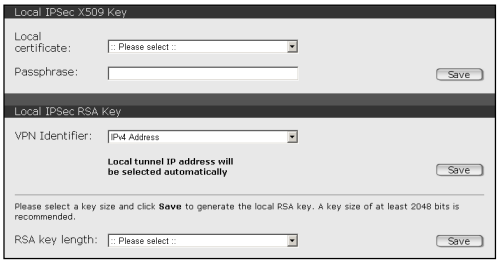
Dieses System unterstützt zur Zeit nur den Deflate-Algorithmus.

6. Falls Sie für diese IPSec Policy noch keinen Namen definiert haben, tragen Sie nun im Eingabefeld **Name** einen Namen ein.

7. Erzeugen Sie nun die Policy durch einen Klick auf die Schaltfläche **Add**.

Die neue **Policy** wird anschließend in der Tabelle **IPSec Policies** angezeigt.

5.6.3. Local Keys


Local IPSec X509 Key
Local certificate:
:: Please select ::
Passphrase:
Save
Local IPSec RSA Key
VPN Identifier:
IPv4 Address
Local tunnel IP address will be selected automatically
Save
Please select a key size and click Save to generate the local RSA key. A key size of at least 2048 bits is recommended.
RSA key length:
:: Please select ::
Save

Im Menü **Local Keys** verwalten Sie das lokale **X.509**-Zertifikat für die X.509-Authentifizierung, definieren den Local IPSec Identifier und das locale RSA-(Key)-Schlüssel-Paar für die RSA-Authentifizierung.

Local IPSec X.509 Key

In diesem Fenster können Sie für **X.509**-Zertifikate, die Sie zuvor im Menü **IPSec VPN/CA Management** erstellt haben, die lokalen Schlüssel definieren.
Das Erstellen der X.509-Zertifikate wird in Kapitel 5.6.5 ab Seite 232 beschrieben.

Wenn Sie die **X.509**-Authentifizierung verwenden möchten, wählen Sie im Drop-down-Menü **Local certificate** das Zertifikat aus. In diesem Drop-down-Menü sind nur die Zertifikate verfügbar, bei denen der passende **Private Key** vorhanden ist.
Tragen Sie anschließend in das Eingabefeld **Passphrase** das Passwort ein, mit dem der **Private Key** gesichert ist.

Anschließend wird der **Active Key** mit seinem Namen im Fenster **Local IPSec X.509 Key** angezeigt. Wenn Sie einen neuen Local Key auswählen, wird der alte automatisch ersetzt.

Das Internet-Sicherheitssystem verwendet nun die ID und den Public/Private Key des aktuellen Local X.509 Key zur Identifizierung, Authentifizierung und zur Verschlüsselung des X.509 IPSec Key Exchanges.

RSA Authentication

Für die Authentifizierung mit **RSA** benötigen Sie einen **Local IPSec Identifier** und einen **Local RSA Key**.

Hinweis:

Die Generierung der **RSA Keys** kann je nach gewählter Schlüssellänge und der verwendeten Hardware bis zu mehreren Minuten dauern.

1. Definieren Sie im Fenster **Local IPSec VPN Identifier** einen einzigartigen **VPN Identifier**.

   IPv4 Address: Für statische IP-Adressen.

   Hostname: Für VPN Security Gateways mit dynamischen IP-Adressen.

   E-Mail Address: Für mobile Roadwarrior-Verbindungen.

   Speichern Sie anschließend die Einstellung durch einen Klick auf die Schaltfläche **Save**

2. Generieren Sie im Fenster **Local RSA Key** einen neuen RSA Key, indem Sie im Drop-down-Menü **RSA Key length** die Schlüsselstärke auswählen.

3. Durch einen Klick auf die Schaltfläche **Save** wird nun die Schlüssel-(Key)-Generierung gestartet.

Anschließend wird der aktive **Local RSA Key** mit seinem Namen angezeigt. Wenn Sie einen neuen Local RSA Key generieren, wird der alte automatisch ersetzt.

PSK Authentication

Für die Authentifizierung mit **Preshared Keys (PSK)** werden keine zusätzlichen Einstellungen für den lokalen IPSec Key benötigt.

Während des Schlüsselaustauschs (Key Exchange) wird passend zum verwendeten **IKE Main Mode** nur **IPv4 Address** als IPSec Identifier unterstützt. Die IPSec Identifier werden im **IKE Main Mode** automatisch durch **PSK** verschlüsselt – die Authentifizierung mit **PSK** kann daher nicht verwendet werden. Die IP-

Adressen der IKE-Verbindung werden automatisch als **IPSec Identifier** verwendet.

Den **PSK Key** tragen Sie im Menü **IPSec Policies/Remote Keys** ein. Er wird dann automatisch als **Local PSK Key** eingesetzt.

5.6.4. Remote Keys

Im Menü **Remote Keys** definieren Sie die IPSec-Remote-Key-Objekte. Ein IPSec-Remote-Key-Objekt repräsentiert eine IPSec-Gegenstelle. Diese Gegenstelle kann ein Security-Gateway, ein Host oder auch ein Roadwarrior mit dynamischer IP-Adresse sein.

Ein IPSec-Remote-Key-Objekt enthält drei Parameter:

- Die IKE-Authentifizierungsmethode (PSK/RSA/X.509)
- Die IPSec ID der Gegenstelle (IP/Hostname/E-Mail-Adresse/ Certificate)
- Die Authentifizierungsdaten (Shared Secret mit PSK, Public Key mit RSA, X.509-Zertifikate werden während dem Key Exchange übermittelt)

Für jede IPSec-Gegenstelle muss ein IPSec-Remote-Key-Objekt definiert werden.

IPSec Remote Key definieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Remote Keys**.

   Anschließend wird das Fenster **New Remote IPSec Key** angezeigt.

2. Tragen Sie in das Eingabefeld **Name** einen Namen für den neuen **Remote Key** ein.

3. **Auto Paket Filter** und **Virtual IP Key** sind optionale Funktionen für **Roadwarrior**-Verbindungen. Wenn Sie den IPSec Remote Key für eine Standard-Verbindung konfigurieren, fahren Sie mit Schritt 4 fort.

   Auto Packet Filter: Wenn diese Funktion eingeschaltet ist, werden Paketfilterregeln, die den Datenverkehr zwischen

dem Roadwarrior mit diesem IPSec-Remote-Key-Objekt und dem lokalen Sub-Netzwerk erlauben, automatisch hinzugefügt. Jedes mal, wenn ein Roadwarrior mit seinem Remote Key erfolgreich einen IPSec-Tunnel aufgebaut hat, bekommt er automatisch Zugang zum lokalen Sub-Netzwerk oder Host.

Das lokale Sub-Netzwerk (**Local Subnet**) oder den Host wählen Sie im Menü **IPSec VPN/Connections** aus.

Sicherheitshinweis:

Wenn Sie die Security Policy konsequent durchführen möchten, schalten Sie die Funktion **Auto Packet Filter** aus und setzen stattdessen die entsprechende Paketfilterregel im Menü **Packet Filter/ Rules**.

Virtual IP key: Mit dieser Funktion können Sie einem Roadwarrior eine virtuelle IP-Adresse zuweisen. Dies ist die einzige Methode eine virtuelle IP-Adresse manuell auszutauschen. Wenn Sie in das Eingabefeld eine IP-Adresse eintragen, dann muss diese auch auf dem Roadwarrior eingetragen werden.

Wichtiger Hinweis:

Die Funktion Virtual IP Key muss verwendet werden, wenn Sie für den IPSec-Tunnel mit einem Roadwarrior die Funktion **NAT Traversal** einschalten.
Die hier eingetragene IP-Adresse darf sonst nirgends verwendet werden und darf nicht Teil eines angeschlossenen Sub-Netzwerks sein.

4. Wählen Sie im Drop-down-Menü **Key type** die IKE-Authentifizierungsart aus. Die weiteren Einstellungen richten sich nach dem ausgewählten **Key type**.

   PSK: Während des Key Exchange wird passend zum verwendeten **IKE Main Mode** nur **IPv4 Address** als **VPN Identifier** der Gegenstelle unterstützt. Tragen Sie in das Eingabefeld **Preshared Key** ein Passwort ein.
   Falls Sie mehrere Roadwarrior-Verbindung konfigurieren möchten, benötigen Sie für alle Verbindungen nur einen PSK.

Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35$4. Stellen Sie sicher, dass dieses Passwort nicht in unbefugte Hände fällt. Der Inhaber dieses Passworts kann damit eine VPN-Verbindung in das geschützte Netzwerk aufbauen. Es ist empfehlenswert das Passwort in regelmäßigen Abständen zu wechseln.

RSA: Das Schlüsselpaar besteht aus einem **Privat Key** und einem **Public Key**. Damit Sie mit der Gegenstelle kommunizieren können, müssen Sie jeweils die **Public Keys** austauschen. Der Austausch der **Public Keys** kann per E-Mail erfolgen.

Wählen Sie im Drop-down-Menü **VPN Identifier** den VPN-ID-Type der Gegenstelle aus. Bei den Optionen **E-Mail Address**, **Full qualified domain name** und **IP Address** müssen Sie die zugehörige Adresse oder den Namen in das darunter liegende Eingabefeld eintragen.

X.509: Wählen Sie im Drop-down-Menü **VPN Identifier** den VPN-ID-Type aus. Bei den Optionen **E-Mail Address**, **Full qualified Domain Name** oder **IP Address** müssen Sie die zugehörige Adresse oder den Namen in das darunter liegende Eingabefeld eintragen.
Für den VPN-ID-Type **Distinguished Name** benötigen Sie die folgenden Daten aus dem X.509-Verzeichnisbaum: Country (C), State (ST), Local (L), Organization (O), Unit (UO), Common Name (CN) und E-Mail Address (E-Mai).

Hinweis:

Beachten Sie zum Aufbau eines X.500-Verzeichnisses auch den Leitfaden **Directory Services** unter der Internetadresse **http://docs.astaro.org**.

5. Um das neue IPSec-Remote-Key-Objekt zu übernehmen, klicken Sie auf die Schaltfläche **Add**.

Das neue IPSec-Remote-Key-Objekt wird anschließend in der Tabelle **Remote Keys** angezeigt.

Die **CA Management Remote Keys** werden in einer separaten Tabelle angezeigt.

5.6.5. CA Management

Certificate Authority (CA) ist die Ausgabestelle von Zertifikaten für öffentliche Schlüssel. Im Menü **CA Management** können Sie Ihre eigene **X.509 Certificate Authority (CA)** erstellen und verwalten. Diese werden bei einer IPSec-Verbindung zur Authentifizierung der Benutzer an den beiden Gegenstellen verwendet. Die dafür verwendeten Informationen sind in den X.509-Zertifikaten gespeichert.
Sie können aber auch Zertifikate verwenden, die von kommerziellen Anbietern, z. B. VeriSign signiert wurden.

Hinweis:

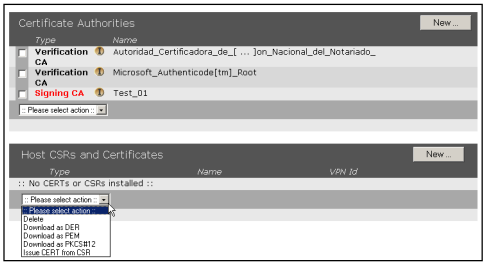
Jedes Zertifikat ist in der **CA** hinsichtlich der darin verwendeten Informationen (Name, Firma, Ort, usw.) eindeutig. Es kann kein zweites Zertifikat mit dem gleichen Inhalt erzeugt werden - auch nicht, wenn das Erste zuvor gelöscht wurde.

Mit dem Menü **CA Management** sind Sie in der Lage, drei verschiedene Zertifikats-Typen zu verwalten. Diese können wiederum für verschiedene Zwecke eingesetzt werden. Dies hängt davon ab, ob jeweils der **Private Key** mit abgespeichert wurde:

CA (Certificate Authority) Certificate: Wenn ein **CA** ohne **Private Key** gespeichert wird, kann dieses bei ankommenden IPSec-Verbindungen zur Authentifizierungsüberprüfung des Host- und Benutzer-Zertifikats verwendet werden. Ein solches **CA** wird als **Verification CA** bezeichnet.
Wenn im **CA** ein **Private Key** vorhanden ist, kann es zum Signieren von Zertifikatsanfragen verwendet werden, um daraus ein gültiges Zertifikat zu erstellen. Dieses **CA** wird dann **Signing CA** genannt.
Auf Ihrem System können mehrere **Verfication CAs** vorhanden sein, allerdings nur ein **Signing CA**.

Host CSR (Certificate Signing Request): Dies ist eine Zertifikats-Anfrage von einem Host. Wenn Sie die Anfrage mit einem **Signing CA** signieren, wird der **Host CSR** zu einem gültigen Host-Zertifikat.

Host Certificate: Das Zertifikat beinhaltet den **Public Key** des Hosts sowie Informationen durch die der Host identifiziert wird, z. B. die IP-Adresse oder den Benutzer. Das Zertifikat ist außerdem durch eine **CA** signiert, die sicherstellt, dass der **Key** auch tatsächlich zu den angegebenen Informationen passt. Dieses gültige Zertifikat wird zur Authentifizierung eines Remote IPSec Hosts/Benutzers verwendet.



Mit Hilfe des Drop-down-Menüs in der Fußzeile der Tabellen können Sie die Zertifikate in verschiedenen Dateiformaten auf Ihren lokalen Client herunterladen oder Zertifikate auf dem System löschen:

PEM: Ein ASCII-codiertes Format. Das Zertifikat bzw. die Anfrage und der Private Key werden in separaten Dateien gespeichert.

DER: Ein binärcodiertes Format. Das Zertifikat bzw. die Anfrage und der Private Key werden in separaten Dateien gespeichert.

PKCS#12: Ein Container-File. Diese Datei kann das Zertifikat, den Private Key und den Authentication CA beinhalten.

Delete: Die ausgewählten Zertifikate werden aus der Tabelle gelöscht.

Issue CERT from CSR: Mit dieser Funktion wird aus dem **CSR** das Zertifikat generiert.

Client/Host-Zertifikat erstellen:

Schritt 1: Das **Signing CA** erstellen.

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **CA Management**.

2. Klicken Sie in der Tabelle **Certificate Authorities** auf die Schaltfläche **New**.

   Anschließend öffnet sich das Fenster **Add Certificate Authority**.

3. Wählen Sie die Option **Generate** aus.

4. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen** für das Zertifikat.
   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

5. Tragen Sie in das Eingabefeld **Passphrase** ein Passwort mit mindestens vier Zeichen ein.

6. Wählen Sie im Drop-down-Menü **Key Size** die Verschlüsselungsstärke aus.

7. Tragen Sie in die Drop-down-Menüs und Eingabefelder **Country** bis **E-Mail Address** die Authentifizierungsdaten für dieses **CA** ein.

8. Um die Einträge zu speichern Klicken Sie auf die Schaltfläche **Start**.

Anschließend wird die **Signing CA** in die Tabelle **Certificate Authorities** geladen. Diese CA wird nun dazu verwendet, um Zertifikats-Anträge (**CSR**) zu signieren und dann daraus ein Zertifikat zu erstellen.

Schritt 2: Den **Zertifikats-Antrag (Request)** erstellen.

1. Klicken Sie in der Tabelle **Host CSR or Certificate** auf die Schaltfläche **New**.

   Anschließend öffnet sich das Fenster **Add Host CSR or Certificate**.

2. Wählen Sie die Option **Generate CSR** aus.

3. Wählen Sie im Drop-down-Menü **VPN ID** den VPN-ID-Type aus.
   Bei den Optionen **E-Mail Address**, **Hostname** und **Ipv4 Address** müssen Sie den zugehörigen Wert in das rechte Eingabefeld eintragen.
   Bei der Option **X.509 DN** bleibt das rechte Feld leer.

4. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen** für den Zertifikats-Antrag.
   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

5. Tragen Sie in das Eingabefeld **Passphrase** ein Passwort mit mindestens vier Zeichen ein.

6. Wählen Sie im Drop-down-Menü **Key Size** die Verschlüsselungsstärke aus.

7. Tragen Sie in die Drop-down-Menüs und Eingabefelder **Country** bis **E-Mail Address** die Authentifizierungsdaten für dieses **CSR** ein.

   Common Name: Wenn Sie dieses CSR für eine Roadwarrior-Verbing erstellen möchten, tragen Sie in dieses Feld den Namen des Benutzers (User) ein. Für die Verbindung zu einem Host tragen Sie hier den Hostnamen ein.

8. Um die Einträge zu speichern klicken Sie auf die Schaltfläche **Start**.

Anschließend wird der Zertifikats-Antrag **CSR + KEY** in die Tabelle **Host CSRs and Certificates** geladen. In der Tabelle wird der Type, der Name und die VPN ID angezeigt. Diese Anfrage kann nun mit der **Signing CA** aus Schritt 1 signiert werden.

Schritt 3: Das Zertifikat erstellen.

1. Wählen Sie in der Tabelle **Host CSRs and Certificates** den neu erstellten Zertifikats-Antrag **CSR + KEY** aus.

2. Wählen Sie im Drop-down-Menü in der Fußzeile der Tabelle die Funktion **Issue CERT from CSR** aus.

   Anschließend wird das Eingabefeld **Signing CA Passphrase** sichtbar. Tragen Sie hier das Passwort der **Signing CA** ein.

3. Klicken Sie auf die Schaltfläche **Start**.

Anschießend wird aus dem Antrag **CSR + KEY** das fertige Zertifikat **CERT + KEY** erstellt und in der Tabelle entsprechend ausgetauscht.

Schritt 4: Zertifikat herunterladen.

1. Wählen Sie in der Tabelle **Host CSRs and Certificates** das neue Zertifikat aus.

2. Wählen Sie im Drop-down-Menü in der Fußzeile der Tabelle ein Download-Format aus.

   DER: Tragen Sie in das Eingabefeld **Passphrase** das Passwort des **Privat Key** ein.

PEM: Für dieses Format wird kein Passwort benötigt.

PKCS#12: Tragen Sie in das Eingabefeld **Passphrase** das Passwort des **Private Key** ein. In das Eingabefeld **Export Pass** geben Sie ein zusätzliches Passwort ein. Dieses Passwort benötigen Sie oder ein anderer Benutzer, um das Zertifikat auf dem externen Client zu importieren.

3. Klicken Sie auf die Schaltfläche **Start**.

Das Zertifikat muss nun auf dem externen IPSec VPN-Client installiert werden. Der Installationsablauf hängt von der IPSec-Software ab, die auf diesem Client verwendet wird.

5.7. System Management (Reporting)

Über das **Reporting** können Sie sich im Internet-Sicherheitssystem aktuelle Systeminformationen und Systemzustände anzeigen lassen sowie verschiedene Protokollfunktionen in Echtzeit öffnen.

Alle Diagramme im Verzeichnis **Reporting** zeigen im ersten Schritt einen Überblick der tagesaktuellen Auslastung. Durch einen Klick auf die Schaltfläche **more** oder auf die jeweilige Grafik öffnen Sie ein Zusatzfenster mit den wöchentlichen, monatlichen oder jährlichen Durchschnittswerten.
Mit einem Klick auf die Schaltfläche **back** gelangen Sie wieder in die aktuelle Übersicht. Die Inhalte der Tabellen können in vier verschiedenen Größen angezeigt werden. Die Größe ändern Sie mit dem Drop-down-Menü **Front size**.

5.7.1. Hardware

CPU utilization - Overview of the day
more...
CPU utilization
Maximum: 55% Average: 21% Current: 24%
RAM utilization - Overview of the day
more...
Free RAM
Maximum: 51252 kb Average: 44631 kb Current: 47172 kb
SWAP utilization - Overview of the day
more...
SWAP in MB
Maximum: 55399 kb Average: 48239 kb Current: 53614 kb

In diesem Menü werden die aktuellen Werte Ihrer System-Hardware angezeigt. Die verfügbaren Werte sind die CPU-Auslastung sowie die RAM und SWAP-Auslastung.

Die Grafiken werden alle fünf Minuten aktualisiert. Die Funktion wird nicht durch jeden Browser unterstützt. In diesem Fall kann das Menü durch einen Klick auf die Schaltfläche **Aktualisieren (Reload)** Ihres Browsers aktualisiert werden.

CPU Utilisation: Das Diagramm zeigt die aktuelle Auslastung des Prozessors durch das Internet-Sicherheitssystem an.

RAM Utilisation: Hier wird die Gesamtsumme des genutzten Hauptspeichers dargestellt. Je mehr Funktionen zur selben Zeit ausgeführt werden, umso weniger Hauptspeicher steht zur Verfügung.

SWAP Utilisation: Das Diagramm stellt die aktuelle Nutzung des virtuellen Speichers dar. Verfügt Ihr System über sehr wenig Arbeitsspeicher (**RAM**) wird die SWAP-Nutzung stark ansteigen.

Harddisk Usage: In der Tabelle wird die Partition der Systemdaten und der jeweilige Speicherplatz auf der Festplatte angezeigt.

Process List: In der Baumstruktur werden die aktuellen Prozesse auf dem Internet-Sicherheitssystem dargestellt.

5.7.2. Network

Intern - Network traffic - Overview of the day
more...
Bits per second
External Interface - Network traffic - Overview of the day
more...
Bits per second
DMZ - Network traffic - Overview of the day
more...
Bits per second

In diesem Menü wird die Datenverkehr-Auslastung der einzelnen Netzwerkkarten grafisch dargestellt. Voraussetzung für dieses Reporting ist, dass alle Netzwerkkarten unter **Network/Interfaces** korrekt konfiguriert wurden.
Die Konfiguration der Netzwerkkarten wird in Kapitel 5.3.1 ab Seite 104 beschrieben.

System Interfaces: In dieser Tabelle werden alle konfigurierten externen und internen Schnittstellen aufgeführt.

Routing Table: In diesem Fenster wird die komplette Routing-Tabelle Ihres Systems dargestellt. Besonders relevant sind die Spalten **Destination**, **Gateway** und **Iface** (Interface).
Destination ist die Adresse des Zielsystems, **Gateway** ist die Adresse des Routers und **Interface** gibt den Namen der eigenen Schnittstelle an, über die das Paket verschickt werden soll.
Die Routen der Netzwerkkarten werden per Default eingetragen und können nicht editiert werden.
Weitere manuelle Einträge werden im Menü **Network/Routing** durchgeführt (Sehen Sie dazu das Kapitel 5.3.2 ab Seite 133).

Arp Table: Diese Tabelle stellt den ARP-Cache des Systems dar. Dies sind alle dem System bekannten Zuordnungen von IP-Adressen zu Hardware-Adressen (MAC).

Network Connections: In der Tabelle werden alle aktuellen Netzwerkverbindung von Ihrem System angezeigt. Verbindungen durch das System werden nicht angezeigt.

5.7.3. HTTP Proxy Cache

HTTP Cache Objects - Overview of the day
more...
Cache Object
Maximum: 98763 Average: 91213 Current: 98763
HTTP object hits - Overview of the day
more...
Object hits in %
Maximum: 90 Average: 41 Current: 35
HTTP memory hits - Overview of the day
more...
Memory hits in %
Maximum: 93 Average: 14 Current: 5

In diesem Menü werden die Werte zur Auslastung des **HTTP-Proxy** (Web) verarbeitet und angezeigt.

Das Diagramm **HTTP Cache Objects** stellt grafisch dar, wieviel Objekte, z. B. HTML-Seiten oder Bilder im HTTP-Proxy gespeichert wurden.

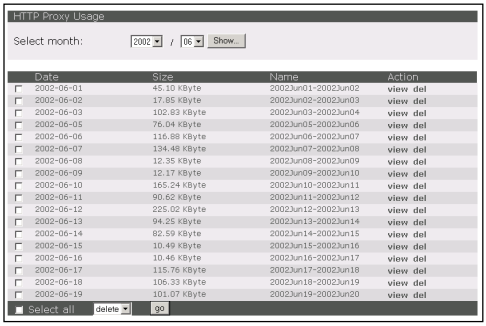
Das Diagramm **HTTP Object Hits** stellt in einer Grafik den prozentualen Anteil aller durch den HTTP-Proxy beantworteten Anfragen (HITs) dar.
Eine Anfrage von einem Browser wird beantwortet, wenn das entsprechende Objekt im Cache des HTTP-Proxys verfügbar und zudem aktuell ist. Dies wird bei jeder Anfrage geprüft.

Im Diagramm **HTTP Memory Hits** wird prozentual dargestellt, wie viel von den lokal gespeicherten Objekten vom HTTP-Proxy direkt aus dem Arbeitsspeicher beantworten wurden.

Wichtiger Hinweis:

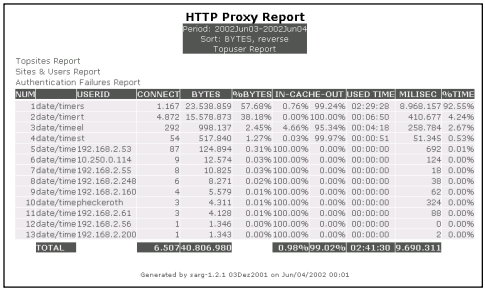
Für dieses Reporting muss der **HTTP-Proxy** eingeschaltet sein, sonst wird in den Diagrammen nur eine gerade, waagerechte Linie dargestellt.

5.7.4. HTTP Proxy Usage



Der Zugriff auf den **HTTP-Proxy** wird vom System detailliert protokolliert. Wenn Sie z. B. den Zugriff eines Clients auf den HTTP-Proxy nur durch den **User Authentication-Modus** erlauben, können Protokolle benutzerspezifisch dargestellt werden.

Die Konfiguration des **HTTP-Proxy** wird in Kapitel 5.5.1 ab Seite 174 beschrieben.



Die Protokolle (Reports) werden einmal am Tag in Form von HTML-Seiten generiert. Das erste Protokoll ist ein Tag nach dem Einschalten und dem ersten Gebrauch des HTTP-Proxy verfügbar. Die Tagesprotokolle können anschließend über die jeweilige Monatsübersicht geöffnet werden.

Im Tagesprotokoll wird für jeden Benutzer (USERID) eine Zeile mit den aufsummierten Datenpaketen (BYTES) erstellt. In diesem Tagesprotokoll können Sie wiederum durch einen Klick auf die Benutzernamen und IP-Adressen weitere Protokolle öffnen, und so detaillierte Informationen über den Zugriff auf den HTTP-Proxy von diesem Client aus erhalten.

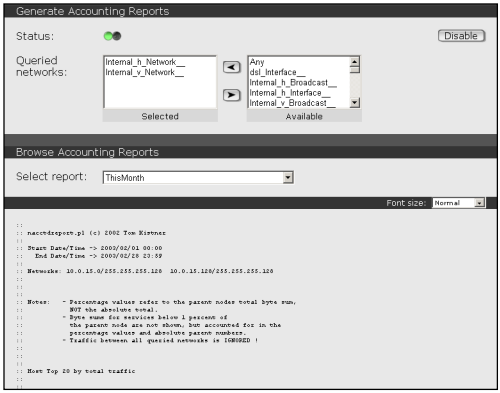
Monatsübersicht laden: Um eine bestimmte Protokollübersicht zu öffnen, wählen Sie mit dem Drop-down-Menü **Select month** das Jahr und den Monat aus und klicken Sie anschließend auf die Schaltfläche **Show**.

Die Protokolle werden anschließend in der darrunterliegenden Tabelle angezeigt.

Protokoll öffnen: Durch einen Klick auf die Schaltfläche **view** wird ein Fenster mit dem Protokoll dieses Tages geöffnet.

Protokoll löschen: Durch einen Klick auf die Schaltfläche **del** wird das Protokoll aus der Tabelle gelöscht.
Mit Hilfe der Optionsfelder und Drop-down-Menü in der Fußzeile der Tabelle können Sie mehrere Protokolle auf einmal löschen. Markieren Sie dafür die entsprechende Zeile durch einen Klick auf das Optionsfeld. Wählen Sie anschließend im Drop-down-Menü **delete** aus und klicken Sie auf die Schaltfläche **go**.

5.7.5. Accounting



Mit dem **Accounting** werden auf den Netzwerkkarten alle IP-Pakete erfasst und ihre Größe einmal am Tag aufsummiert. Zusätzlich wird zu Beginn eines Monats die Datensumme des vergangenen Monats berechnet. Das Ergebnis wird in einem Protokoll ausgegeben. Die Summe dient z. B. als Basis für den Betrag, den Ihnen Ihr Internet Service Provider in Rechnung stellt, wenn Sie Ihre Verbindung nach übertragenem Datenvolumen bezahlen.

Das **Accounting** wird im Menü **Network/Accounting** eingeschaltet und konfiguriert. Die Konfiguration dieser Funktion wird im Kapitel 5.3.8 ab Seite 158 beschrieben.

Browse Accounting Reports: In diesem Fenster werden vorhandenen Accounting-Protokolle angezeigt. Mit dem Drop-down-Menü **Select report** wählen Sie den Monat aus. Das Protokoll wird anschließend im darrunterliegenden Fenster angezeigt.

Im Menü **Log Files/Accounting** können die Protokolle auf Ihren lokalen Rechner heruntergeladen oder gelöscht werden.

Report for current Month: In diesem Fenster wird das Accounting-Protokoll des aktuellen Monats angezeigt.

Accounting definieren:

1. Öffnen Sie im Verzeichnis **Reporting** das Menü **Accounting**.

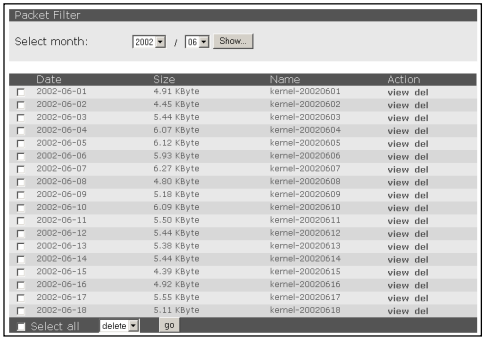
2. Schalten Sie die Funktion **Accounting Reports** durch einem Klick auf die Schaltfläche **Enable** ein.

3. Wählen Sie im Auswahlfeld unter dem Fenster **Queried networks** die Netzwerke aus, für die ein detailliertes Protokoll erstellt werden soll. In der Regel ist dies Ihr LAN- und/ oder das DMZ-Netzwerk.

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 35 beschrieben.

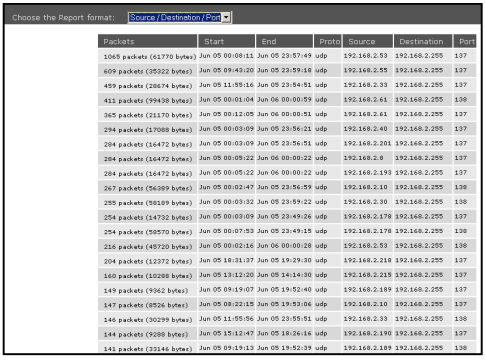
Die Netzwerke werden sofort übernommen und erscheinen anschließend im Fenster **Queried networks**.

5.7.6. Packet Filter


Packet Filter
Select month:
2002 / 06 Show..
Date Size Name Action
2002-06-01 4.91 KByte kernel-20020601 view del
2002-06-02 4.45 KByte kernel-20020602 view del
2002-06-03 5.44 KByte kernel-20020603 view del
2002-06-04 6.07 KByte kernel-20020604 view del
2002-06-05 6.12 KByte kernel-20020605 view del
2002-06-06 5.93 KByte kernel-20020606 view del
2002-06-07 6.27 KByte kernel-20020607 view del
2002-06-08 4.80 KByte kernel-20020608 view del
2002-06-09 5.18 KByte kernel-20020609 view del
2002-06-10 6.09 KByte kernel-20020610 view del
2002-06-11 5.50 KByte kernel-20020611 view del
2002-06-12 5.44 KByte kernel-20020612 view del
2002-06-13 5.38 KByte kernel-20020613 view del
2002-06-14 5.44 KByte kernel-20020614 view del
2002-06-15 4.39 KByte kernel-20020615 view del
2002-06-16 4.92 KByte kernel-20020616 view del
2002-06-17 5.55 KByte kernel-20020617 view del
2002-06-18 5.11 KByte kernel-20020618 view del
Select all delete go

In dieser Übersicht sind die Protokolle zu **Packet Filter** enthalten, wobei hier nur die geblockten Pakete protokolliert werden. Die Protokolle werden in Form von HTML-Seiten dargestellt und werden einmal am Tag generiert.

Durch einen Klick auf die Schaltfläche **view** wird das Tagesprotokoll geöffnet.



Mit dem Drop-down-Menü in der Kopfzeile können Sie dieses Tagesprotokoll nach bestimmten Kriterien darstellen. Die Spalten **Packets** (Datenpaketgröße in Bytes), **Start** (Beginn der Regelverletzung), **End** (Ende der Regelverletzung) und **Proto** (Protokoll) werden immer dargestellt.
In der linken Übersicht wurden z. B. die Spalten **Source**,

Destination und **Port** ausgewählt. Falls mehrere Verletzungen mit derselben Quell- und Zieladresse und denselben Ports stattfanden, wird in der Spalte **Start** der Zeitpunkt der ersten und in der Spalte **End** der Zeitpunkt der letzten Verletzung angegeben.

Weitere Funktionen

Protokoll einsehen: Durch einen Klick auf die Schaltfläche **view** wird ein Fenster mit dem Bericht dieses Tages geöffnet.

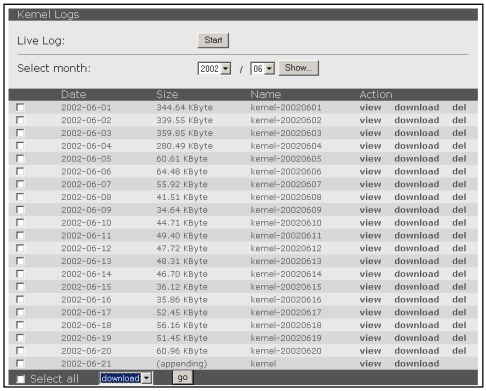
Protokoll löschen: Durch einen Klick auf die Schaltfläche **del** wird der Eintrag aus der Tabelle gelöscht.

Mit Hilfe der Optionsfelder und dem Drop-down-Menü in der Fußzeile der Tabelle können Sie mehrere Protokolle auf einmal löschen. Markieren Sie dafür die entsprechende Zeile durch einen Klick auf das Optionsfeld. Wählen Sie anschließend im Drop-down-Menü **delete** aus und klicken Sie auf die Schaltfläche **go**.

5.8. Log Files (Log Files)

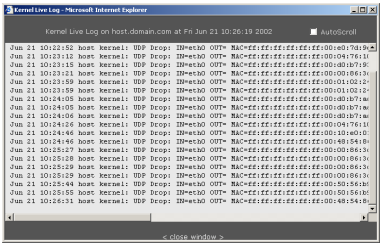
Über **Log Files** können Sie sich die vom System archivierten Protokolle anzeigen lassen. Mit Ausnahme von **Accounting** und **WELF** können die Protokollfunktionen mit **Live Log** in Echtzeit beobachtet werden.

Alle Protokoll-(Log File)-Übersichten im Verzeichnis **Log Files** sind gleich aufgebaut und beinhalten bis auf wenige Ausnahmen die gleichen Funktionen.


Kernel Logs
Live Log:
Start
Select month:
2002
06
Show...
Date
Size
Name
Action
2002-06-01 344.64 KByte kernel-20020601 view download del
2002-06-02 339.55 KByte kernel-20020602 view download del
2002-06-03 359.85 KByte kernel-20020603 view download del
2002-06-04 280.49 KByte kernel-20020604 view download del
2002-06-05 60.61 KByte kernel-20020605 view download del
2002-06-06 64.48 KByte kernel-20020606 view download del
2002-06-07 55.92 KByte kernel-20020607 view download del
2002-06-08 41.51 KByte kernel-20020608 view download del
2002-06-09 34.64 KByte kernel-20020609 view download del
2002-06-10 44.71 KByte kernel-20020610 view download del
2002-06-11 49.40 KByte kernel-20020611 view download del
2002-06-12 47.72 KByte kernel-20020612 view download del
2002-06-13 48.31 KByte kernel-20020613 view download del
2002-06-14 46.70 KByte kernel-20020614 view download del
2002-06-15 36.12 KByte kernel-20020615 view download del
2002-06-16 35.86 KByte kernel-20020616 view download del
2002-06-17 52.45 KByte kernel-20020617 view download del
2002-06-18 56.16 KByte kernel-20020618 view download del
2002-06-19 51.45 KByte kernel-20020619 view download del
2002-06-20 60.96 KByte kernel-20020620 view download del
2002-06-21 (appending) kernel view download
Select all
download
go

Beim Öffnen einer Protokoll-(Log File)-Übersicht wird immer der aktuelle Monat angezeigt (siehe Bild links).

Live Log: Das heutige Protokoll kann durch einen Klick auf die Schaltfläche **Start** geöffnet werden (siehe Bild unten).



In der Monatsübersicht ist dieses Protokoll mit dem Vermerk **appending** in der letzten Zeile vermerkt.

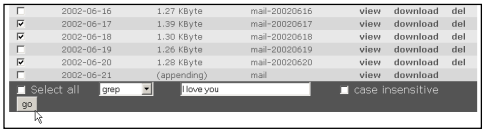
Select month: Um eine bestimmte Protokollübersicht zu öffnen, wählen Sie mit diesen Drop-down-Menüs das Jahr und den Monat aus und klicken anschließend auf die Schaltfläche **Show**.

View: Durch einen Klick auf diese Schaltfläche wird ein Fenster mit dem Protokoll des entsprechenden Tages geöffnet.

Del: Durch einen Klick auf diese Schaltfläche wird das Protokoll aus der Tabelle gelöscht.

Download: Durch einen Klick auf diese Schaltfläche können Sie die **Log Files** auf Ihren lokalen Client herunterladen. Diese **Log Files** können anschließend zur Auswertung der Daten in externe Programme z. B. Microsoft Excel importiert werden.

Mit Hilfe der Optionsfelder und dem Drop-down-Menü in der Fußzeile der Tabelle können Sie mehrere **Log Files** auf einmal herunterladen (**download**) oder löschen (**delete**). Markieren Sie dafür die entsprechende Zeile durch einen Klick auf das Optionsfeld. Wählen Sie anschließend im Drop-down-Menü die Funktion aus und klicken Sie auf die Schaltfläche **go**.


2002-06-16 1.27 KByte mail-20020616 view download del
2002-06-17 1.39 KByte mail-20020617 view download del
2002-06-18 1.30 KByte mail-20020618 view download del
2002-06-19 1.26 KByte mail-20020619 view download del
2002-06-20 1.28 KByte mail-20020620 view download del
2002-06-21 (appending) mail view download
Select all
grep
I love you
case insensitive
go

Grep: Mit dieser Funktion können Sie in den **Log Files** nach bestimmten Zeichenketten (Strings) suchen. Wählen Sie in der Monatsübersicht zuerst die **Log Files** aus, in denen nach der Zeichenkette gesucht werden soll, und wählen Sie dann im Drop-down-Menü die Funktion **grep** aus. Anschließend öffnet sich das Eingabefeld. Tragen Sie hier die Zeichenkette ein. Durch einen Klick auf das Optionsfeld **case insensitive** wird die Groß-/Kleinschreibung bei der Suche ignoriert. Starten Sie anschließend den Suchvorgang durch einen Klick auf die Schaltfläche **go**.

Nach Beendigung des Suchvorgangs werden alle gefundenen Zeilen mit dieser Zeichenkette in einer Tabelle dargestellt. Falls keine Zeile mit dieser Zeichenkette enthalten ist, wird ein leeres Fenster angezeigt.

5.8.1. Kernel

In den **Kernel**-Logs wird der System-Status protokolliert, inklusive der Meldungen von den Gerätetreibern, der Meldung des Boot-Prozesses sowie der vom Paketfilter (Packet Filter) geblockten Datenpakete.

5.8.2. SMTP Relay

In den **SMTP Relay**-Logs werden die Aktivitäten des SMTP-Dienstes protokolliert. Alle eingehenden E-Mails werden darin aufgeführt. Zusätzlich werden alle Unregelmäßigkeiten, z. B. zugewiesene **Bounce**-Stati, Ausfälle oder blockierte E-Mails protokolliert.

5.8.3. HTTP Proxy

In den **HTTP Proxy**-Logs werden die Aktivitäten von HTTP-Clients protokolliert.

Im Menü **Reporting/HTTP Proxy Usage** werden die protokollierten Daten ausgewertet und strukturiert in Form von HTML-Seiten dargestellt.
Das Menü **HTTP Proxy Usage** wird in Kapitel 5.7.4 ab Seite 240 beschrieben.

5.8.4. Packet Filter

In den **Packet Filter**-Logs werden alle geblockten Datenpakete protokolliert. Diese Log Files sind ein Teil der Kernel-Logs.

5.8.5. PPTP Roadwarrior Access

In den PPTP-Logs wird der Verlauf beim Zugriff des externen Clients auf das System protokolliert. Dies beinhaltet das Einloggen und die Authentifizierung sowie eventuelle Fehler beim Verbindungsaufbau.

Wenn Sie im Menü **Network/PPTP Roadwarrior Access** für die Funktion **Logging** den Parameter **Extensive** eingestellt haben, werden im PPTP-Log auch ausführliche Informationen zur PPP-Verbindung angezeigt.

5.8.6. IPSec VPN

In den IPSec-Logs werden umfangreiche Informationen zu den Einstellungen der IPSec-Verbindung protokolliert. Dies beinhaltet auch Informationen zum Schlüsselaustausch (Key Exchange) und zur Verschlüsselung (Encryption).

5.8.7. Daemon

In diesen generischen **Log Files** werden verschiedene Informationen zu Daemon-Prozessen auf dem Internet-Sicherheitssystem protokolliert. Dies beinhaltet den SOCKS-Proxy, den Authentication-Deamon, den SuperDaemon und den DNS-Server.

5.8.8. Selfmonitor

Das **Selfmonitoring** gewährleistet die Systemintegrität des Internet-Sicherheitssystems und setzt den Administrator über wichtige Ereignisse in Kenntnis. Das Selfmonitoring überwacht die Funktion, Performance und Sicherheit der relevanten System-Parameter und greift bei Abweichungen, die über eine gewisse Toleranz hinausgehen, regulierend ein. Anschließend erhält der zuständige Administrator per E-Mail einen Bericht.

Das **Selfmonitoring** des Internet-Sicherheitssystems stellt sicher, dass zentrale Dienste z. B. der Syslog Daemon, der HTTP-Proxy oder das Network-Accounting ordnungsgemäß funktionieren.
Zugriffsrechte auf Dateien werden ebenso überwacht wie der Anteil einzelner Prozesse am Verbrauch der Systemresourcen, wodurch eine eventuelle Überlastung des Systems bereits im Vorfeld verhindert wird. Darüber hinaus erhält der Systemverwalter rechtzeitig Hinweise auf sich abzeichnende Ressourcen-Engpässe, wenn z. B. der verfügbare Festplattenspeicher knapp werden sollte. Erforderliche Maßnahmen zur Systemerweiterung bzw. Entlastung können so rechtzeitig geplant werden.

5.8.9. Portscan

Das Portscan-System erkennt Portscans und benachrichtigt den Administrator per E-Mail. Wenn Sie die **Log Files** in diesem Menü analysieren, ziehen Sie keine voreiligen Schlüsse hinsichtlich der in diesen Protokollen angegebenen Quelladresse (SRC - IP Source Address) und dem Quell-Port (SPT – Source Port). Diese Angaben können vom eigentlichen Absender leicht gefälscht werden. Nützliche Informationen erhält man durch die Auswertung der Ziel-Adresse (DST – Destination IP Adresses) und des Ziel-Portes (DPT – Destination Port).

Die Funktion **Portscan Detection** wird im Menü **Network/ Portscan Detection** eingeschaltet und konfiguriert.

Die **Administrator E-Mail-Adresse** richten Sie im Menü **System/Settings** ein.

5.8.10. Admin Access

In diesen **Log Files** werden Informationen zu Einlogg-Prozessen ins Konfigurationstool **WebAdmin**, ins Remote Shell oder in die lokale Konsole protokolliert.

5.8.11. Notification

In den **Notification-Log Files** werden alle **Notification-E-Mails**, die durch das Internet-Sicherheitssystem abgeschickt wurden, protokolliert. Auf diese Weise kann der Administrator auch kritische Systemvorgänge beobachten, wenn ihn keine Notification E-Mails erreicht haben.

Hier sind alle Fehler-, Warnungs- und Informations-Codes aufgeführt:

INF:

```
000         System was restarted

            Das System wurde neu gestartet (gebootet).

010         Backup file

            Eine Backup-Datei wurde vom System automa-
            tisch generiert und per E-Mail an den Admi-
            nistrator verschickt.

050         No new System Up2Dates available

            Das System ist auf dem aktuellsten Stand.

051         System Up2Dates successfully fetched

            Eine oder meherere System Up2Dates wurden
            auf das System geladen, aber noch nicht in-
            stalliert. Die System-Up2Date-Daten sind im
            E-Mail-Text aufgeführt.

052         System Up2Dates successfully installed

            Ein oder mehrere System Up2Dates wurden er-
            folgreich auf dem System installiert.
            Die System-Up2Date-Daten sind im E-Mail-Text
            aufgeführt.
```

053 No new version in file://var/recovery/incoming

Es sind keine installierbaren Up2Date-Pakete vorhanden.

054 New Pattern have been installed

Ein oder mehrere Pattern Up2Dates wurden installiert. Die Pattern-Up2Date-Daten sind im E-Mail-Text aufgeführt.

060 POP3 scanner has denied a message

Der POP3-Scanner hat eine eingehende E-Mail gefiltert. Die E-Mail können Sie im Proxy Content Manager einsehen. Der Proxy Content Manager wird im Kapitel 5.5.7 ab Seite 205 beschrieben.

070 Daily log rotate found a 'core' file - noted

Eine Core-Datei wurde gefunden. Diese wird nach sieben Tagen automatisch gelöscht. Falls eine Core-Datei öfters gefunden wird, wenden Sie sich an den Support Ihres Sicherheitssystem-Anbieters.

Selfmonitornachrichten:

101 Signature check hanging – stopped

102 WebAdmin not running – restarted

103 Kernel log daemon not running – restarted

104 Accounting not running – restarted

105 Accounting not running – restarted

106 HTTP proxy not running – restarted

107 Syslog not running – restarted

108 MiddleWare not running – restarted

109 not running – restarted

110 Portscan detection watch not running - restarted

111 SNMP not running – restarted

112 Nameserver not running – restarted

113 Incorrect /tmp permission - set to correct

114 RX buffer error on network card – rebooting

115 SelfMonitor restart requested – restarted

116 Licenseserver not running – restarted

117 dynamic IPSec Packetfilter watch not running – restarted

118 Surf Protection not running – restarted

119 HTTP proxy not responding – restarted

120 Authentication server not running – restarted

121 High Availability version conflict – Updating Slave

Auf dem Firewall-System im Hot-Standby-Modus (Slave) wurde das letzte System-Up2Date-Paket noch nicht installiert. Die Installation wurde nun ausgeführt.

122 High Availability version conflict – noted

Auf dem Firewall-System im Hot-Standby-Modus (Slave) fehlt mehr als ein System-Up2Date-Paket. Spielen Sie die fehlenden System-Up2Date-Pakete in das Internet-Sicherheits-system ein und installieren Sie diese anschließend.
Das Modul Up2Date Service wird in Kapitel 5.1.3 ab Seite 52 erklärt.

123 High Availability version conflict – Starting reboot

Die Version des Firewall-Systems im Hot-Standby-Modus (Slave) ist höher als die Version des Firewall-Systems im Normal-Modus (Master). Das High-Availability-System wird nun neu gestartet. Das Firewall-System mit

der höheren Version wird anschließend den Normal-Modus (Master) übernehmen.

WAR:

000 Demoversion expiring - obtain a valid license

Die 30 Tage-Demo-Lizenz ist abgelaufen.

005 To many log files – will be deleted automatically soon

Auf der Festplatte sind zu viele Log Files enthalten. Diese Log Files nehmen auf der Festplatte zuviel Platz ein. Die ältesten Log Files werden in Kürze automatisch gelöscht.

006 To many log files – oldest ones have been deleted

Auf der Festplatte waren zu viele Log Files enthalten. Diese Log Files haben auf der Festplatte zuviel Platz eingenommen. Die ältesten Log Files wurden automatisch gelöscht.

007 Portscan detected from <IP>

Es wurde ein Portscan entdeckt, der von der angegebenen IP-Adresse aus gestartet wurde. Welche Maßnahmen gegen den Angreifer eingeleitet werden hängt von den Einstellungen im Menü Portscan Detection ab. Das Modul wird im Kapitel 5.3.5 ab Seite 145 erklärt.

030 Virus detected, admin message

In einer E-Mail wurde ein Virus entdeckt. Eine entsprechende Mitteilung wird an die E-Mail-Adresse des Postmasters gesendet.

031 Blocked mail due to RegExp

In einer E-Mail wurde eine unerwünschte String-Folge entdeckt. Die E-Mail wird nicht an die Empfängeradresse gesendet. Der Absen-

der der E-Mail erhält eine entsprechende Nachricht.

032 Blocked mail due to content type (file extension)

In einer E-Mail wurde ein Anhang (Attachment) mit einer unerwünschten Erweiterung (Extension) entdeckt. Die E-Mail wird nicht an die Empfängeradresse gesendet. Der Absender der E-Mail erhält eine entsprechende Nachricht.

033 Virus detected, sender message

In einer E-Mail wurde ein Virus entdeckt. Der Absender der E-Mail erhält eine entsprechende Nachricht.

034 Virus detected, rcpt message

In einer E-Mail wurde ein Virus entdeckt. Der Empfänger der E-Mail erhält eine entsprechende Nachricht. Per Default-Einstellung wird diese E-Mail allerdings nicht an den Empfänger abgeschickt.

035 Mail delivery failed

Eine E-Mail kann wegen eines andauernden Fehlers nicht an die Empfängeradresse gesendet werden, bzw. das Zeitintervall in der das System versucht die E-Mail an den Empfänger weiterzuleiten ist abgelaufen. Der Absender der E-Mail erhält eine entsprechende Nachricht.

036 Mail delivery deferred

Eine E-Mail kann wegen eines vorübergehenden Fehlers nicht an die Empfängeradresse gesendet werden. Der Absender der E-Mail erhält eine entsprechende Nachricht. Das System versucht nun innerhalb eines bestimmten Zeitintervalls die E-Mail an die Empfängeradresse weiterzuleiten.
Nach Ablauf des Zeitintervalls erfolgt die Meldung WAR 035.

060 Surf Protection remote database connection failure – retrying

Beim Remote-Zugriff auf die Surf-Protection-Datenbank ist ein Fehler aufgetreten. Die Verbindung wird neu gestartet.

080 HA check: no link beat on interface – retrying

Die Überwachung des Firewall-Systems im Normal-Modus mittels Link Beat ist fehlgeschlagen. Der Versuch wird neu gestartet. Falls die Funktionen nach mehreren Versuchen nicht gestartet werden kann, erhält der Administrator die Notification-E-Mail WAR 081.
Falls Sie für das HA-System diese Überwachungsfunktion nicht einsetzen, müssen Sie keine weiteren Schritte einleiten. Nachdem vom Internet-Sicherheitssystem die Nachricht WAR 081 verschickt wurde, erfolgt kein weiterer Versuch mehr, die Überwachung mittels Link Beat zu starten.

081 HA check: interface does not support link beat check

Die Funktion zur Überwachung des Firewall-Systems im Normal-Modus mittels Link Beat konnte trotz mehrer Versuche nicht gestartet werden.
Falls es sich hierbei um eine Neuinstallation des HA-Systems handelt und Sie die Überwachung mittels Link Beat beabsichtigen, vergewissern Sie sich bitte, dass die Netzwerkkarten vom Internet-Sicherheitssystem unterstützt werden. Des Weiteren prüfen Sie bitte auf beiden Firewall-Systemen ob für die Datentransfer-Verbindung die link-beat-fähige Netzwerkkarte ausgewählt wurde.
Die Installation und die Funktionsweise des HA-Systems wird in Kapitel 5.1.8 ab Seite 89 erklärt.

100 Not enough free space on harddisk - please check

Auf der Festplatte steht nicht mehr genügend freier Speicherplatz zur Verfügung.

101 System load to high - please check

Öffnen Sie im Verzeichnis Reporting die folgenden Systeminformationen und prüfen die laufenden Prozesse:

Hardware: Prüfen Sie alle Werte in diesem Menü, z. B. Prozessor (CPU), Arbeitsspeicher (RAM), belegter Speicher auf der Festplatte (SWAP) etc.

Network: Prüfen Sie die Anzahl der Verbindungen und den Datenverkehr auf den Schnittstellen.

Öffnen Sie im Verzeichnis Log Files die Menüs Kernel und Daemon und prüfen die Protokolle auf Auffälligkeiten.

Sollten Sie die Ursache nicht finden, stellen Sie die folgenden Daten zusammen und wenden Sie sich an den Support Ihres Sicherheitssystem-Anbieters: Hardware-Kenndaten, die Versionsnummer des Sicherheitssystems, die Notification-Mails und die obigen Werte und Daten.

102 Too much memory for a single process - please check

Für einen einzelnen Prozess wurde zuviel Arbeitsspeicher (RAM) benötigt. Gehen Sie in diesem Fall wie bei der Nachricht WAR 101 beschrieben vor.

103 Allocating to much swap - please check

Es wurde für einen oder mehrere Prozesse zuviel Platz auf der Festplatte (SWAP) zugeteilt. Gehen Sie in diesem Fall wie bei der Nachricht WAR 101 beschrieben vor.

104 High Availability slave device not found - please check

Das Firewall-System 2 im Hot-Standby-Modus (Slave) wurde nicht gefunden.
Die Installation und die Funktionsweise des HA-Systems wird in Kapitel 5.1.8 ab Seite 89 erklärt.

105 No accounting config file - ignored

200 Failed login from <IP> as <Username>

Von der angegebenen IP-Adresse aus wurde unter dem angegebenen Benutzernamen ein Versuch unternommen, sich am Internet-Sicherheitssystem anzumelden. Der Versuch ist fehlgeschlagen.

ERR:

000 No update possible.
Failed to connect available Update Server

Der Up2Date-Server ist nicht erreichbar.
Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

001 Up2Date Package is corrupted - downloading again

Es kann vorkommen, dass ein Up2Date-Paket nach dem Download defekt (die Prüfsumme stimmt nicht) ist. Bitte laden Sie die Datei dann nochmals herunter. Falls das Problem dann noch besteht, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

002 No ssh keys found under $SSH_KNOWN_HOSTS

Der Versuch diesen Up2Date-Server zu benutzen ist fehlgeschlagen, da für den Server kein SSH Host Key vorhanden ist. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

003 No space left for System Update

Ein System Update konnte wegen zu geringem Festplattenspeicher nicht durchgeführt werden. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

Support-Fälle:

004 System Up2Date to new version failed
- Internal Error

Das System Update ist fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

005 System Up2Date to new version failed
- Internal Error

Das System Update ist fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

006 System Up2Date to new version failed
- Internal Error

Das System Update ist fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

007 System Up2Date to new version failed
- Internal Error

Das System Update ist fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

008 Failed to connect available Up2Date Server for Pattern Up2Date

Der Up2Date-Server ist nicht erreichbar. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

009 Failed to start Virus Scanner. Please repeat Pattern Up2Date

Der Virus Scanner konnte nicht gestartet werden. Starten Sie die Funktion Pattern Up2Date neu.
Falls das Problem weiterhin auftritt setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

010 Please repeat Pattern Up2Date

Die neuen Pattern Up2Dates wurden nicht installiert, der Virenscanner läuft mit den bisher installierten Pattern.
Falls das Problem öfter auftritt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

5.8.12. Accounting

In diesem Menü sind alle vom System archivierten **Accounting**-Protokolle verfügbar. In dieser Übersicht können diese Protokolle als **ASCII**- oder **CSV**-Dateien heruntergeladen oder gelöscht werden. Im Menü **Reporting/Accounting** können die Protokolle betrachtet werden.

In den **ASCII**-Dateien sind die einzelnen Werte durch Tabulatoren voneinander getrennt und folgendermaßen aufgebaut:

```
[timestamp][proto][src_addr][src_port][dst_addr][dst_port][bytecount]
```

timestamp: Ein UNIX-Zeitstempel, angegeben in Sekunden seit dem 1. Januar 1970.

proto: Die IP-Subprotokollnummer.

src_addr und **src_port**: Die Quell-Adresse und der Quell-Port des gezählten Datenpakets.

dst_addr und **dst_port**: Die Ziel-Adresse und der Ziel-Port des gezählten Datenpakets.

bytecount: Die gesamte Datengröße dieser Verbindung in Bytes inklusive des Headers und eventueller Füllbytes.

Die **CSV**-Datei ist genau wie die ASCII-Datei aufgebaut. Die Werte sind hier allerdings durch Semikolons voneinander getrennt. Auf diese Weise können diese Dateien in Microsoft Excel leicht importiert werden.

Das **Accounting** wird im Menü **Network/Accounting** eingeschalten und konfiguriert. Die Konfiguration dieser Funktion wird im Kapitel 5.3.8 ab Seite 158 beschrieben.

5.8.13. WELF

Die **WELF**-Log Files (Webtrends Enhanced Logfile Format) können in das Auswertungs-Tool **WebTrends Logfile Analysis Suite** importiert werden. Die WELF-Log Files enthalten die protokollierten Paketfilter-Verletzungen. Diese können mit WebTrends analytisch dargestellt werden.

Ausführliche Informationen zu WebTrends erhalten Sie unter folgender Internetadresse:

http://www.webtrends.com

5.8.14. POP3

In den **POP3**-Logs werden die Aktivitäten des POP3-Dienstes protokolliert. Alle ausgehenden E-Mails werden darin aufgeführt. Zusätzlich werden alle Unregelmäßigkeiten, z. B. Ausfälle oder blockierte E-Mails protokolliert.

5.9. Die Hilfe-Funktionen (Help)

Im Menü **Help** stehen Ihnen neben **Online Help** drei weitere Funktionen zur Verfügung.

Search

Mit Hilfe dieser Funktion wird im **WebAdmin** und in **Online Help** nach dem von Ihnen eingegebenen Begriff gesucht und der Begriff wird in einem separaten Fenster angezeigt.

Suche starten:

1. Öffnen Sie im Verzeichnis **Help** das Menü **Search**.
2. Geben Sie in das Eingabefeld **Search term** den Begriff ein.
3. Bestimmen Sie im Auswahl wie viel Begriffe angezeigt werden sollen.
4. Um die Suche zu starten, klicken Sie auf die Schaltfläche **seek**.

Falls der Begriff im **WebAdmin** oder in **Online Help** geführt wird, liefert das Ergebnis folgende Infos:

Pfad zur entsprechenden Funktion im **WebAdmin**

Link zum gesuchten Begriff in **Online Help**

Kurze Info zur im Pfad angezeigten Seite im **WebAdmin**

Index

Hier sind alle Menüs alphabetisch geordnet. Der angegebene Pfad gibt an, wo die entsprechende Funktion im **WebAdmin** zu finden ist. Durch einen Klick auf den Begriff wird **Online Help** gestartet und Sie gelangen direkt zur entsprechenden Information.

Glossary

In diesem Verzeichnis entspricht die Struktur der Begriffe ihrer Zuteilung im **WebAdmin**. Durch einen Klick auf die Begriffe erhalten Sie einen Überblick der Funktionen in diesem Verzeichnis.

5.10. Firewall verlassen (Exit)

Wenn sie den Browser mit einer offenen **WebAdmin**-Session schließen ohne den **WebAdmin** über **Exit** zu verlassen, so bleibt die letzte Session bis zum Ablauf des Time-outs aktiv.
In solch einem Fall können Sie sich erneut am **WebAdmin** anmelden. Es wird ein Bildschirm angezeigt, der Sie darüber informiert, dass bereits ein anderer Administrator eingeloggt ist. Sie können mit der Schaltfläche **Kick** die andere Session beenden und sich selbst wieder einloggen. Falls Sie damit die WebAdmin-Session eines anderen Administrators beenden, sollten sie im Eingabefeld für „Type reason here" den Grund für die Übernahme der Session angeben.

6. Zusätzliche Funktionen

6.1. Serielle Konsole

Falls Sie nicht die **High Availability (HA)**-Lösung installiert haben, kann an das Internet-Sicherheitssystem über die serielle Schnittstelle COM 1 eine serielle Konsole angeschlossen werden. Hierfür können Sie z. B. das Terminalprogramm **Hyperterminal** verwenden, das in den meisten Microsoft Windows-Versionen bereits enthalten ist. Für die Verbindung zwischen der Konsole und dem Sicherheitssystem benötigen Sie ein Nullmodem-Kabel.

Die erforderlichen Anschlusseinstellungen sind:

Bits pro Sekunde: **9600**, Datenbits: **8**, Parität: **N** (keine), Stoppbits: **1**.

Per Default ist der Zugang über die serielle Schnittstelle deaktiviert.

Serielle Schnittstelle für serielle Konsole aktivieren:

1. Loggen Sie sich als **Shell Administrator user** ein.

   Benutzernamen: **root**

   Password: Passwort des Shell Administrator-Benutzers

2. Geben Sie folgende Zeile ein und bestätigen Sie dies mit der **Enter**-Taste:

   joe /etc/inittab

3. Scrollen Sie zum Abschnitt **Serial login** und editieren Sie diese zu folgenden Zeilen:

   # Serial login
   # modify it if you want a console on serial port
   s0:123:respawn:/sbin/mgetty ttyS0

4. Speichern Sie die Änderungen mit der folgenden Tastenkombination:

   Ctrl-K X

5. Geben Sie folgende Zeile ein und bestätigen Sie dies mit der **Enter**-Taste:

   joe /emergency/boot/etc/lilo.conf

6. Scrollen Sie zum Abschnitt **#serial=0,9600n8** und löschen Sie das **#**-Zeichen:

   serial=0,9600n8

7. Suchen Sie nach einer Zeile mit dem Eintrag **append** und editieren Sie diese zu folgender Zeile:

   append = "acpi=off console=ttyS0,9600n8"

   Falls keine Zeile mit dem Eintrag **append** vorhanden ist, scrollen Sie an das Ende der Datei und fügen eingerückt die folgende Zeile ein:

   append = "console=ttyS0,9600n8"

8. Speichern Sie die Änderungen mit der folgenden Tastenkombination:

   Ctrl-K X

9. Geben Sie den folgenden Befehl ein und bestätigen Sie dies mit der **Enter**-Taste:

   lilo -r /emergency/boot

10. Geben Sie den folgenden Befehl ein und bestätigen Sie dies mit der **Enter**-Taste:

    kill -1 1

Anschließend ist die serielle Schnittstelle am Internet-Sicherheitssystem als Zugang für eine serielle Konsole aktiviert.

6.2. Factory Reset

Mit **Factory Reset** wird das Internet-Sicherheitssystem in den ursprünglichen Zustand nach der Installation zurückgesetzt, d. h. alle Daten, die nach der Installation auf dem System erzeugt oder eingegeben wurden, werden gelöscht. Dies betrifft insbesondere die gesamte Konfiguration, den **HTTP Proxy Cache**, die **E-Mail Queues**, die **Accounting**- und **Reporting**-Daten, alle Passwörter und alle noch nicht installierten **Up2Dates**.
Der Versionsstand des Internet-Sicherheitssystems bleibt erhalten, alle installierten **System Up2Dates** und **Pattern Up2Dates** werden nicht verändert.

Factory Reset:

1. Loggen Sie sich als **Shell Administrator user** ein.

   Benutzernamen: **root**.

   Password: Passwort des Shell Administrator-Benutzers

2. Geben Sie über die Konsole folgende Zeile ein und bestätigen Sie dies mit der **Enter**-Taste:

   cd /sbin/init.d

3. Geben Sie über die Konsole folgende Zeile ein und bestätigen Sie dies mit der **Enter**-Taste:

   ./factory_reset reset

4. Beantworten Sie die Sicherheitsabfrage mit **yes**.

   Alle laufenden Prozesse und Programme werden beendet. Das **Factory Reset** wird durchgeführt und das Internet-Sicherheitssystem in den Halt-Zustand gefahren:

   Die LED-Anzeige **SCROLL** auf der Tastatur blinkt, und es ertönen Beeps im Sekundentakt.

5. Führen Sie einen Hardware-Reset durch (**Strg** + **Alt** + **Entf** oder **Reset**).

Nach dem Neustart wird die interne Netzwerkkarte mit der bei der Installation festgelegten Konfiguration initialisiert. Im Konfigurationstool **WebAdmin** müssen nun alle Passwörter neu gesetzt und die System-Konfiguration neu erstellt werden.

Backups können, soweit die Version der im Backup enthaltenen Konfigurations-Daten dafür vorgesehen sind, installiert werden.

Glossar

Broadcast

Die Adresse, an die sich ein Rechner wendet, wenn er alle Rechner im gleichen Subnetz ansprechen will.
Beispiel: Bei einem Netzwerk mit der IP-Adresse 212.6.145.0 und der Netzmaske 255.255.255.240 wäre ein Broadcast die Adresse 212.6.145.15.

Client

Ein Client ist ein Programm, das über ein Netzwerk mit einem Server kommuniziert um den von ihm zur Verfügung gestellten Dienst zu nutzt.
Beispiel: Netscape ist ein WWW-Client, mit dessen Hilfe man Informationen von einem WWW-Server abrufen kann.

Client-Server Prinzip

Nach dem Client-Server Prinzip gestaltete Anwendungen verwenden auf der Benutzerseite ein Clientprogramm (Client), das mit einem bestimmten Dienstrechner im Netz (Server) Daten austauscht. Der Server ist dabei i.d.R. für die Datenhaltung zuständig, während der Client die Präsentation dieser Daten und die Interaktion mit dem Benutzer übernimmt. Dazu bedienen sich Client und Server eines genau definierten Protokolls. Alle wichtigen Anwendungen im Internet (z.B. WWW, FTP, News) basieren auf dem Client-Server Prinzip.

DNS

Dank des Domain Name Systems (auch: Domain Name Service) kann der Anwender statt der rechnerfreundlichen IP-Nummer den menschenfreundlicheren Namen, bzw. Aliase, verwenden. Für die Umsetzung von Nummer nach Name sorgen die Nameserver. Jede am Internet angeschlossene Institution muss mindestens zwei voneinander unabhängige Nameserver betreiben, die über Namen und Nummern dieser Institution Auskunft geben können. Zusätzlich gibt es für jede Top-Level Domain

einen Nameserver, der über eine Liste aller nachgeordneten Nameserver dieser Domain verfügt.

Das Domain Name System stellt also eine verteilte, hierarchische Datenbank dar. Im Normalfall fragt jedoch nicht der Benutzer selbst die Datenbank ab, sondern die Netzanwendung (z. B. Netscape) mit der er gerade arbeitet.

Dual-Homed Gateway

Man geht von einer Maschine ohne IP-Forwarding aus, die mit einem Netzwerkinterface Kontakt zum lokalen Netzwerk bzw. zum internen Teil einer Firewall besitzt und die mit einem zweiten Netzwerkinterface mit dem externen Teil einer Firewall bzw. dem Internet verbunden ist. Aufgrund des fehlenden IP-Forwarding müssen alle Verbindungen über dieses Dual-Homed Gateway weitergeleitet werden.

Firewall

Eine Firewall dient der Abschirmung und damit dem Schutz eines (Teil-) Netzwerks (z. B. Astaro) von einem anderen Netzwerk (z. B. dem Internet). Der gesamte Netzwerkverkehr geht über die Firewall, wo er reguliert und reglementiert werden kann.

Header

Im Allgemeinen ein Bereich am Anfang bzw. am Kopf von Dateien, in dem grundsätzliche Informationen über diese Datei gespeichert sind. Im Speziellen ist es der Teil einer E-Mail oder einer Usenet-Nachricht, die Informationen über Inhalt, Absender und Datum gibt.

Host

In Client-Server-Architekturen bezeichnet man als Host den Rechner, auf dem die Server-Software läuft. Dabei können auf einem Host mehrere Server laufen, zum Beispiel ein FTP- und ein E-Mail-Server. Auf einen Host kann man mit Hilfe von Clients zugreifen, zum Beispiel mit einem Browser oder einem E-Mail-Programm.
Da der Ausdruck **Server** außer für das entsprechende Programm (also die Software) auch für den Rechner verwendet wird, auf

dem das Programm läuft (also die Hardware), wird in der Praxis nicht klar zwischen Server und Host unterschieden.

In der Datenfernübertragung bezeichnet man denjenigen Rechner als Host, von dem Daten (wie FTP-Dateien, News, WWW-Seiten) abgerufen werden. Ein Host wird im Internet auch als **Node** (Knoten) bezeichnet.
Auf einem Internet-Host (im Unterschied zum **Localhost**) kann man (zum Beispiel über Telnet) auch aus der Ferne arbeiten (Remote Access).

ICMP

Neben dem **IP-Protokoll** gibt es eine Variante mit speziellen Funktionen. Das **Internet Control Message Protocol (ICMP)** wird zur Übermittlung von Kontrollinformationen zwischen aktiven Netzwerkkomponenten oder Rechnern verwendet. Den meisten Anwendern sind die ICMP-Typen Echo (Typ 8) und Echo Reply (Typ 0) im Zusammenhang mit dem Programm **ping** bekannt.
Empfängt ein Rechner ein ICMP-Echo-Paket, so muss sein IP-Stack ein ICMP-Reply-Paket an den Absender zurückschicken. Man macht dies mit dem Programm ping, um festzustellen, ob eine andere Netzwerkkomponente über IP zu erreichen ist.

IP

Das **Internet Protocol** ist das Basisprotokoll für die Datenübertragung im Internet, das seit 1974 nahezu unverändert in Gebrauch ist. Es regelt den Verbindungsauf- und -abbau sowie die Fehlerkennung. Durch Verwendung von **NAT** und **Masquerading** können private Netzwerke auf offizielle IP-Adressen gemappt werden – auf diese Weise wird der Ipv4-Adressraum noch lange ausreichen.

IP-Adresse

Jeder Host besitzt eine eindeutige IP-Adresse, vergleichbar mit einer Telefonnummer. Eine IP-Adresse besteht aus vier durch Punkte voneinander getrennte dezimale Ziffern. Die möglichen Ziffern sind 0 bis einschließlich 255.
Beispiel: Eine mögliche IP-Adresse ist 212.6.145.1.

Zu jeder IP-Adresse gehört mindestens ein IP-Name der Form `hostname[[.subdomain]s].domain`, z. B. `kises.rz.uni-konstanz.de`. Hiermit wird ein Rechner namens `kises` bezeichnet, der in der Sub-Domain `rz` der Sub-Domain `uni-konstanz` der Domain `de` steht. Wie bei IP-Adressen, werden die einzelnen Namensteile durch einen Punkt voneinander getrennt. Anders als bei IP-Adressen jedoch, sind IP-Namen nicht auf vier Stellen beschränkt. Außerdem können einer IP-Adresse mehrere IP-Namen zugeordnet sein, man spricht dann von Aliasen.

Masquerading

Dynamisches **Masquerading** bezeichnet das Verbergen interner Netzwerkinformationen (LAN) nach außen.

Beispiel: Der Rechner eines Mitarbeiters mit der IP-Adresse 212.6.145.100 steht in einem maskierten Netzwerk. Allen Rechnern in seinem Netzwerk wird eine einzige, offizielle IP-Adresse zugeordnet, d. h. wenn er nun eine HTTP-Anfrage in das Internet startet, wird seine IP-Adresse durch die IP-Adresse der externen Netzwerkkarte ersetzt.
Damit enthält das ins externe Netzwerk (Internet) gehende Datenpaket keine internen Informationen. Die Antwort auf die Anfrage wird von der Firewall erkannt und auf den anfragenden Rechner weitergeleitet.

nslookup

Ein Unix Programm zur Abfrage von Nameservern. Die Hauptanwendung ist die Anzeige von IP-Namen bei gegebener IP-Nummer, bzw. umgekehrt. Darüber hinaus können aber auch noch andere Informationen wie z.B. Aliase angezeigt werden.

Port

Während auf IP-Ebene nur die Absender- und Zieladressen zur Übertragung verwendet werden, müssen für TCP und UDP weitere Merkmale eingeführt werden, die eine Unterscheidung der einzelnen Verbindungen zwischen zwei Rechnern erlauben. Dies sind die Portnummern. Eine Verbindung auf TCP und UDP-Ebene ist damit durch die Absenderadresse und den Absenderport sowie die Zieladresse und den Zielport eindeutig identifiziert.

Protokoll

Ein Protokoll ist ein klar definierter und standardisierter Satz von Regeln, mit deren Hilfe ein Client und ein Server miteinander kommunizieren können. Bekannte Protokolle und die damit betriebenen Dienste sind z. B. HTTP (WWW), FTP (FTP) und NTP (News).

Proxy (Application Gateway)

Die Aufgabe eines Proxy (Application Gateways) ist die vollständige Trennung von Kommunikationsverbindungen zwischen dem externen Netzwerk (Internet) und dem internen Netzwerk (LAN). Zwischen einem internen System und einem externem Rechner kann keine direkte Verbindung existieren.
Die Proxies arbeiten vollständig auf der Applikationsebene. Firewalls, die auf Proxies basieren, benutzen ein Dual-Homed Gateway, das keine IP-Pakete weiterleitet. Die Proxies, die auf dem Gateway als spezialisierte Programme ablaufen, können nun Verbindungen für ein spezielles Protokoll entgegennehmen, die übertragenen Daten auf Applikationsebene verarbeiten und anschließend weiterleiten.

RADIUS

RADIUS steht für Remote Authentication Dial In User Service. RADIUS ist ein Protokoll, mit dem ein Router Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen kann.

Router (Gateway)

Ein Router ist ein Vermittlungsrechner, der eine intelligente Wegewahl für die Netzwerkpakete auswählt. Ein Gateway ist streng genommen etwas anderes als ein Router, aber im Zusammenhang mit TCP/IP sind beide Begriffe synonym. Wenn man Verbindungen über das eigene Netzwerk hinaus aufbauen möchte, muss man dem eigenen Rechner diesen Router (Gateway) bekannt machen. Gewöhnlich wird die höchste oder die niedrigste Adresse verwendet, z. B. im Netzwerk 192.168.179.0/24 die Adresse 192.168.179.254 oder 192.168.179.1.

Server

Ein Server ist ein Rechner im Netz, der besondere, i.d.R. standardisierte, Dienste anbietet, z.B. WWW, FTP, News, usw. Um diese Dienste nutzen zu können, brauchen Sie als Anwender einen für den gewünschten Dienst passenden Client.

SOCKS

SOCKS ist ein Proxyprotokoll, das dem Anwender erlaubt, eine Punkt-zu-Punkt-Verbindung zwischen einem internem und einem externem Rechner über das Internet zu erstellen. SOCKS, oft auch Firewall Transversal Protocol genannt, existiert derzeit in der Version 5 und klinkt sich auf Clientseite in die SOCKS-Aufrufe der Programme ein.

Subnet Mask

Die Subnet Mask oder Netzmaske gibt an, in welche Gruppen die IP-Adressen eingeteilt sind. Aufgrund dieser Einteilung werden einzelne Rechner einem Netzwerk zugeordnet.

UNC-Pfad

Mit Hilfe eines **Universal Naming Convention**-Pfadnamen (UNC-Pfad), z. B. \\Servername\Freigabename kann man manuell eine Verknüpfung zu einem Netzlaufwerk erstellen.

Index

Accounting
  Netzwerk ausschließen .. 159
  Netzwerkkarte hinzufügen/entfernen .. 159
Accounting 158
Administrator e-mail addresses 42
Akustische Signale
  Beep, 5 mal 94
  Endlos-Beep 94
Backup
  Einführung 59
  einspielen 62
  E-Mail Backup File 63
  E-Mail Backup File generieren 63
  E-Mail Backup File verschlüsseln 64
  E-Mail-Adressen bearbeiten 64
  Encryption Backup File 64
  manuell generieren 60
Benutzer
  editieren 103
  Einführung 102
  hinzufügen 102
  löschen 103
Broadcast
  auf ein Netzwerksegment 169
  auf gesamtes Internet ... 168
Certificate, WebAdmin Site ... 86
Connection Tracking 160
DHCP Server
  DNS-Server zuweisen 143
  Einführung 142
  konfigurieren 142
  Leases 144
  Static mappings 144
Dienste
  editieren 100
  Einführung 99
  hinzufügen 99
  löschen 100
Dienstgruppe
  editieren 102
  löschen 102
Dienstgruppen
  definieren 101
  Einführung 101
DNS Proxy
  konfigurieren 183
Exit 260
Factory Reset 263
Fehler
  Ursachen 26, 107
Filter Live Log
  Current NAT rules 173
  Current Packet Filter rules 173
  Einführung 172
  Packet Filter Logs 173
General System Settings 42
Glossar
  Broadcast 265
  Client 265
  Client-Server Prinzip 265
  DNS 265
  Dual-Homed Gateway ... 266
  Firewall 266
  Header 266
  Host 266
  ICMP 267
  IP 267
  IP-Adresse 267
  Masquerading 268
  nslookup 268
  Port 268

- Protokoll 269
- Proxy..... 269
- RADIUS 269
- Router 269
- Server 270
- SOCKS..... 270
- Subnet Mask..... 270
- UNC-Pfad 270

Glossary..... 259
High Availability.....89
High Availability-System installieren 90
Hochverfügbarkeit 89
Hostname.....42
HTTP
- Clear Proxy Cache 182
- Content Filter..... 182
- Surf Protection Profiles .. 179

HTTP Proxy
- Surf Protection profile .. 180, 181
- User Authentication-Modus 177

HTTP-Proxy
- konfigurieren 177
- Standard-Modus..... 176
- Transparent-Modus..... 176

ICMP
- Einführung 170
- Firewall forwards ping ... 172
- Firewall forwards traceroute 171
- Firewall is ping visible ... 172
- Firewall is traceroute visible 171
- ICMP forwarding..... 170
- ICMP on firewall 171
- Ping on firewall 172
- Ping Settings 172
- Traceroute on firewall ... 171
- Traceroute Settings 171

Index..... 259
Installation
- Anleitung.....21
- Einführung.....17
- Konfiguration 26
- Software 21
- Version 3.2x auf 4.0 aktualisieren.....17
- Vorbereitung.....21

Interfaces
- Einführung..... 104
- MTU Size..... 132

IPSec VPN
- AH-Protokoll 214
- CA Management 232
- Client/Host-Zertifikat erstellen..... 233
- Connections..... 217
- Einführung..... 209
- Global IPSec Settings 217
- IPSec..... 212
- IPSec Connections 218
- IPSec Live Log 219
- IPSec Modi 213
- IPSec-Protokolle 214
- konfigurieren 220
- Local IPSec X.509 Key... 227
- Local Keys 227
- Manual Keying 215
- Policies 223
- Policy konfigurieren 223
- PSK Authentication 228
- Remote Key definieren .. 229
- Remote Keys 229
- RSA Authentication 228
- Schlüsselverwaltung..... 215
- Transport Modus 213
- Tunnel Modus 213
- VPN Routes..... 218
- VPN Status 218

Licensing 49
Load Balancing
- Regel definieren 140

Regel editieren 141
Regel löschen 141
Load Balancing 140
Log Files
Accounting 257
Admin Access 248
Daemon 246
Fehler-Codes 248
grep 245
HTTP Proxy 246
IPSec VPN 246
Kernel 245
Notification 248
Packet Filter 246
POP3 258
Portscan 247
PPTP Roadwarrior Access 246
Selfmonitor 247
SMTP Relay 245
WELF 258
Masquerading
Regel definieren 139
Regel editieren 139
Regel löschen 139
Masquerading 138
Microsoft Outlook
Regeln erstellen 203
NAT
NAT-Regel definieren 136
Regel editieren 138
Regel löschen 138
NAT 134
Network Groups 97
Networks 96
Netzwerke
editieren 97
Einführung 96
hinzufügen 96
löschen 97
Netzwerkgruppe
editieren 98
löschen 98
Netzwerkgruppen
definieren 98
Einführung 97
Netzwerkkarten
MAC-Adressen ermitteln 115
Wireless LAN Security ... 113
Notification 42
Paketfilterregel
aktiv, inaktiv 167
editieren 168
Einführung 164
löschen 168
Regelsatz-Tabelle sortieren 168
Reihenfolge ändern 168
setzen 166
Pattern Up2Date
installieren, automatisch .. 58
installieren, manuell 58
Ping
Einführung 161
starten 161
POP3
konfigurieren 187
Portscan Detection
Einführung 145
einschalten/ausschalten. 146
Netzwerk ausschließen .. 147
PPTP Roadwarrior Access
Einführung 148
MS Win 2000-Szenario .. 150
PPTP Roadwarrior Network Access 148
PPTP Roadwarrior VPN
Optional Parameters 150
PPTP IP-Pool 149
Protokolle
AH 99, 100
ESP 99, 100
TCP 99
UDP 99
Proxy

DNS 183
Einführung 174
HTTP 174
Ident 189
POP3 187
Proxy Content Manager . 205
SMTP 190
SOCKS 185
Proxy abschalten
MS Explorer 175
Netscape 175
Proxy Content Manager
Delete all content of type 208
Mail-ID 205
pop3 206
smtp_err 205
smtp_queue 205
Type 205
PSD Network Exclusion 147
Qualitiy of Service (QoS) setzen 155
Quality of Service (QoS)
Quality of Service Rules. 156
Quality of Service (QoS) 154
Reporting
Accounting definieren 242
Accounting 241
Hardware 237
HTTP Proxy Cache 239
HTTP Proxy Usage 240
Network 238
Packet Filter 242
Restart 94
Routing
Einführung 133
Kernel Routing Table 134
Rules 164
Schließen automatisch 46
Schnittstellen
Aktuelle Übersicht 106
Einführung 104
Ethernet-Netzwerkkarte. 108
Hardware-Übersicht 107
Link BW 132
PPPoA-DSL einrichten 129
PPPoE-DSL einrichten 126
PPPoE-DSL-Verbindung 125, 128
Proxy ARP 131
QoS Status 131
Resered unshaped Bandwidth 132
Virtual LAN 122
Virtual LAN einrichten 124
Wireless LAN 112
Wireless LAN Access Point einrichten 116
Wireless LAN Station einrichten 119
Zusätzliche Adresse 110
zusätzliche Adresse zuweisen 110
Zusätzliche Einstellungen 131
Search
Suche starten 259
Search 259
Secure Shell 48
Serielle Konsole 261
Service Groups 101
Services 99
Settings 42
Shut down 94
Shut down/Restart 94
SMTP
Antispam/Content Control 195
Encryption/Authentication 193
Global Whitelist 194
SMTP Proxy

konfigurieren 191
SMTP Queue
bounce 206
frozen 206
frozen bounce 206
SMTP Relay
Postmaster address 191
SOCKS Proxy
Benutzerauthentifizierung 186
konfigurieren 185
Statisches Routing
definieren 133
Einführung 133
Syslog
Einführung 65
System Time
automatisch synchronisieren 45
manuell einstellen 44
System Up2Date
einspielen, automatisch ... 54
einspielen, lokal 55
einspielen, manuell 53
installieren 56
installieren auf HA-Lösung 56
Systemvoraussetzungen
Administrations-PC 19
Beispielkonfiguration 19
Hardware 18
TCP Connect
Einführung 162
starten 163
Time Settings 43
Tools 160
Traceroute
Einführung 161
starten 162
Up2Date Service
Einführung 52
Pattern Up2Date 57
System Up2Date 53
Use external indicators 43
User Authentication
Einführung 66
LDAP einstellen 81
LDAP erweitert 84
LDAP Server 73
Microsofts IAS RADIUS einstellen 68
MS Active Directory-Server einstellen 75
Novell eDirectory-Server einstellen 80
OpenLDAP-Server Konfigurieren 81
RADIUS 67
SAM 71
SAM – NT/2000/XP einstellen 71
Users 102
WebAdmin
Auswahlfelder 35
Darstellung 34
Drop-down-Menü 37
Einführung 17, 40
Hide tooltips 34
Hierarchiefeld 37
HTTPS 46
Info-Box 33
Kick 41
Menü 35
Online-Hilfe 39
Pinne 34
starten 41
Statusampel 35
Tooltips 34
Verzeichnis 34
Width 34
WebAdmin TCP Port ändern 46
Zertifikat für WebAdmin
erstellen 87
installieren 87

© Astaro AG